TU Delft
Faculty of Technology, Policy and Management

Master Thesis

"*Trust Service Broker*: A proposal to overcome global distrust in information infrastructures"

Charalampos Karypidis

4187369

Master Thesis Committee

First supervisor:	Dr. Semir Daskapan	ICT section
Second supervisor:	Dr. Laurens Rook	TSE section
Chairman:	Prof. Dr. Jan van den Berg	ICT section

Acknowledgements

I would like to acknowledge and extend my genuine gratitude to the following persons who have made the completion of this Thesis possible:

My First Supervisor, dr. Semir Daskapan, for the opportunity he gave me to expand on his work through this challenging and very interesting topic, for the confidence he has shown in me and also for his significant help in reviewing this work, despite the geographical distance that separated us.

The Chairman of my Thesis committee, prof. dr. Jan van den Berg, for taking out time of his busy schedule in order to provide his assistance whenever I needed it and also for his invaluable feedback throughout the process.

Dr. Christian Doerr, for his kind and significant contribution to this work, even though he could not formally act as my second supervisor.

All the academic and industry experts who were involved in this work, for all the time they took and their contribution.

Finally, I would also like to thank my family and friends for their unconditional support throughout the past seven months.

Abstract

The globalization of economy has significantly increased the role of online information exchange between transacting parties worldwide. Currently implemented trust models, such as Public Key Infrastructure, provide enough means to enable the secure exchange of data, but only within specified territories, thereby forming different trust domains worldwide. Due to technical, organizational and political hindrances, an efficient universal trust model interconnecting different trust domains cannot be established by relying on one of the current archetypes of trust models. In this paper, we propose an Architecture based on an alternative, hybrid trust model in order to deal with the interoperability issues across different trust domains: the Trust Service Broker Architecture. We demonstrate the effectiveness of the TSB in a scenario related to international supply chain operations. We begin by describing a particular logistics case, more specifically an import trade lane from Malaysia to the Netherlands, as well as the issues associated with the information exchange between relevant stakeholders, which subsequently drive the requirements for the TSB architecture. Building on current knowledge, we then present a detailed overview of the TSB architecture and how it can facilitate safe and reliable information exchange for organizations involved in the logistics case. In order to do so, we also present a high level overview of the internal TSB security risks. Finally, we attempt to validate and generalize the TSB solution from a theoretical perspective, while also discussing the results and the implications for future research.

Keywords

Online Trust management, Trust domains, Interoperability, Online security, International Supply Chain, Trust Service Broker, TSB architecture.

Contents

List of Tables

List of Figures

List of Abbreviations

AES Advanced Encryption Standard

AIA - Authority Information Access

AKI - Authority Key Information

API - Application Programming Interface

BCA - Bridge Certificate Authority

CA - Certificate Authority

CRL - Certificate Revocation List

CSR - Certification Request

DB - Database

DC - Digital Certificate

DES - Data Encryption Standard

DFD - Data Flow Diagram

DID - Defense-In-Depth

DMZ - Demilitarized Zone

DNS - Domain Name System

DoS - Denial of Service

DSA - Digital Signature Algorithm

DSRM - Design Science Research Methodology

EDI - Electronic Data Interchange

EPCIS - Electronic Product Code Info System

EU - European Union

FCL - Full Container Load

FF - Freight Forwarder (Seacon's partner)

FOB - Free On Board

FTP - File Transfer Protocol

HBI - High Business Impact

HTTP - HyperText Transfer Protocol

ICT - Information Communication Technology

IP - Internet Protocol

IT - Information Technology

LAN - Local Area Network

LBI - Low Business Impact

LDAP - Lightweight Directory Access Protocol

MAC - Message Authentication Code

MBI - Medium Business Impact

MIME - Multipurpose Internet Mail Extension

MSAT - Microsoft Security Assessment Tool

MYS - Malaysia

NIST - National Institute of Standards & Tech.

NL - The Netherlands

OWL - Web Ontology Language

PCS - Port Community System

PGP - Pretty Good Privacy

PII - Personally Identifiably Information

PKI - Public Key Infrastructure

POR - Point of Reference

RSA - Rivest,Shamir,Adelman (algorithm)

SAI - Subjet Alternative Name

SHA - Secure Hash Algorithm

SKI - Subject Key Information

SMTP - Simple Mail Transfer Protocol

SPKI – Simple Public Key Infrastructure

SRMG - Security Risk Management Guide

MSPF - Multiple Single Points of Failure

SSL - Secure Sockets Layer

TLS - Transport Layer Security

TSB - Trust Service Broker

TTP - Trusted Third Party

UML - Unified Modelling Language

URI - Uniform Resource Identifier

VPN - Virtual Private Network

CHAPTER 1: Introduction

1.1 The trust domains problem

1.1.1 Theoretical perspective

The issue of online trust will be at the core of this Thesis. *Trust* in information infrastructures is defined by (Daskapan, 2005) as "*a relationship between two elements, a set of operations, and a security policy in which element X trusts element Y if and only if X has confidence that Y behaves in a well-defined way that does not violate the given security policy*". As the word trust implies reliance on others, there is no reliability in open networks without reference on third parties. In other words, a key consideration is that trust between two entities in information infrastructures is most often achieved not directly, but rather indirectly through intermediates. Such intermediates that play the role of establishing a trusted relationship between two unrelated entities that do not trust each other directly are called "Points of Reference" (POR) (Daskapan, et al., 2004).

There are various trust models, differing in the way they include these PORs. (Daskapan, et al., 2004) presented four main archetypes of trust models, categorizing them across two main dimensions, namely topology and status. Topology refers to the structure of the end entities (centralized vs. de-centralized), interacting through a Point of Reference. Status refers to the degree of authority (institutionalized vs. anarchistic). An overview of these archetypes of trust models is presented in Table 1.1.

	TOPOLOGY	
STATUS	Central	Decentral
High	Central Hierarchical	Meshed Hierarchical
Low	Central Peer	Decentral Peer

Table 1.1: Archetypes of trust models

The **central hierarchical** archetype refers to the class of trust models, in which trust is derived by referencing to a central institutionalized authority (El-Ashqar, et al., 2012). According to this trust principle, superior entities (authorities) vouch for the end entities (peers) by granting credentials (certificates). Authorities that issue and manage certificates to identify individuals or organizations are called Certificate Authorities. Figure 1.1 presents an overview of this class. As we can see, even though the end entities (peers) may not trust each other directly, they derive their trustworthiness indirectly, by referencing to higher level authorities who provide them with credentials (certificates). In turn, these authorities derive their trustworthiness by a higher level authority and in the root of this "tree", we find the so called Root Certificate Authorities, whose role is usually played by

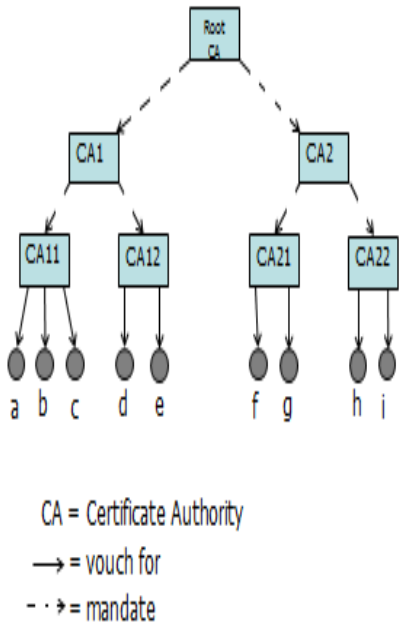

Figure 1.1: Central Hierarchical Models

governments (or government institutions).

The **meshed hierarchical** archetype refers to the class of trust models, where interconnections with otherwise unrelated trust authorities are linked either by a non-hierarchical authority (Bridge Certificate Authority – BCA), or through cross-certification between the CAs (Lopez Millan, et al., 2010). The main difference with the previous model is that the interconnecting authority (BCA) does not derive its trustworthiness through a superior position, but rather by being trusted by both (and perhaps additional) CAs. In other words, there is a two-way verification scheme. Such models are used for interconnecting CAs (decentralized PORs with a high status) in different countries, where a universal root CA does not exist, as we will also discuss later. Figure 1.2 depicts such a model.

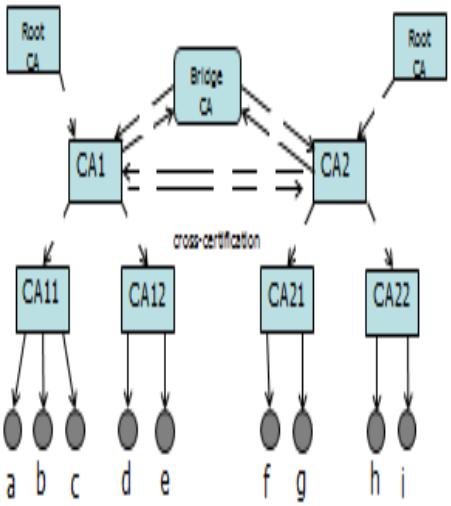

Figure 1.2: Meshed Hierarchical Models

In the **central peer** models, the Point of Reference is centralized, but unlike the Central Hierarchical models, it is not a higher level authority, but has a low status; in other words the POR is just another peer, "privileged" to provide trust. This central peer has the duty of "mediating credentials between all the peers who want to interact with each other". An example of this class is the Kerberos system, where interactions between peers (or "principals" in this case) are first requested from the central POR: a Key Distribution Center and its related Ticket Granting Server (Xiong, 2012). An example of a particular central peer model (Kerberos) is given in figure 1.3.

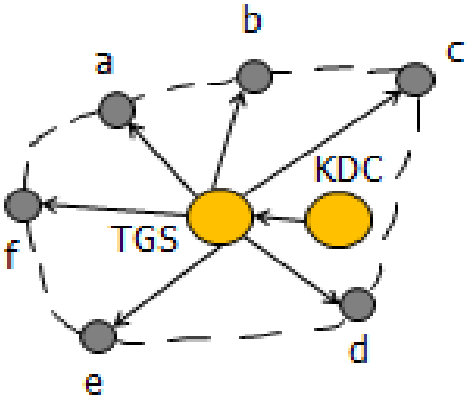

Figure 1.3: Kerberos, an example of a central peer model

Finally, in the **decentralized peer** models, all entities (peers) can act as a Point of Reference. There are neither higher level authorities, nor any superior or centralized peer privileged to issue credentials for the others (like in the central peer model). In that sense, everything depends on *relative* trust between the end entities and each peer can play a double role: either as a communicating peer or as a POR. An overview of this class of trust models is presented in Figure 1.4.

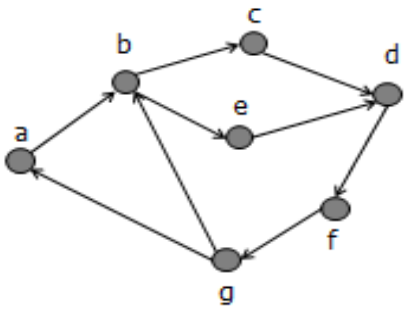

Figure 1.4: Decentralized peer models

Unfortunately, all the aforementioned trust models have some serious limitations regarding their deployment on a worldwide scale. (Daskapan, et al., 2004) discussed the limitations of these models in relation to the issue of global distrust.

The *central hierarchical* model, while highly reliable, is mostly limited for national level trust relationships. The primary reason for this is that there is currently no global Certificate Authority to bind all lower authorities, since there is no consensus for such a

"super-national" Point of Reference. The United Nations could play this role in theory; however it is not recognized by all countries and may be biased. In addition, even if such an authority existed, the hierarchy tree would be very long and, therefore, complexity and manageability issues would arise.

Similar issues arise when we consider a solution through a *central peer* model. Again, a global point of reference does not exist and, in addition, this model would only be sufficient for a limited amount of entities. Moreover, if such a POR existed, it would become too critical, since all authentication processes are controlled by a Key Distribution Centre (i.e. in a Kerberos protocol) and, therefore, if an attacker compromises this authentication infrastructure, he will be able to impersonate any other peer.

Meshed hierarchical models might offer more possibilities to overcome interoperability issues, but they also have limitations. Since agreeing for a Bridge Certificate Authority to interconnect the remote CAs in different countries is a step towards a global point of reference, these models suffer from similar limitations as the central hierarchical ones. In addition, we are now facing two-way verification paths and, consequently, the technical complexity is increased. Finally, trying to deal with this issue through cross-certification between n CAs (one in each domain), would require n(n-1) links, which is not feasible – at least for now – due to technical, social, legal and economic constraints.

Finally, while the *decentralized peer* models can overcome global distrust and interoperability issues, since they respect the anarchy inherent in the internet, they suffer in terms of reliability. Since trust is derived by relations among peers – without an official POR – the truth can be faked. Hence, such models are not recommended for high value transactions, which are common in the context of e-businesses.

In practice, Public Key Infrastructure (PKI), an example of the central hierarchical class of trust models, is often seen as the means to establish a secure communications path for transacting individuals or organizations (Adams & Lloyd, 2002) (El-Ashqar, et al., 2012). In addition, solutions such as the Kerberos Protocol (a central peer model) are widely implemented for security purposes, such as authentication procedures within organizations, and are often integrated with public key cryptography, as in Cross Realm Authentication protocols (Xiong, 2012). However, as already discussed, such models can provide the answer to electronic security only within specified domains. For instance, PKI is normally implemented within national boundaries and the provision of a secure communications path between organizations in different regions is limited.

Finally, nowadays perhaps the most common practical implementation of inter-domain PKI comes at the form of root CA certificates being embedded into popular web browsers. However, although this is a workable approach, it still suffers from two main drawbacks. First, and perhaps most importantly, end entities are "forced" to trust the certificates of CAs that might reside in other regions of the world without any direct trust relationship present. And second, there are issues related to the efficient manageability of certificates, with research pointing out that the process of updating the contents of embedded CA certificates is quite difficult and inefficient (Pala & Smith, 2010).

To conclude, the issue at the core of this research can be defined as follows: "***There exists no universal trust model to efficiently provide a secure communications path across different trust domains worldwide".***

At this point it is important to clarify that *the trust domains problem is a generic one, since the definition of a "domain" is not only limited to different countries, but it can also relate to different trust models, even within the same country*, for instance Public Key Infrastructure to PGP web of trust.

1.1.2 Practical (business) implications

In contemporary times, technology increasingly plays a role of paramount importance in how people communicate and do business. The Internet is used to store, inform and communicate data on a daily basis. Despite this fact, however, it is still constrained by security concerns. Every individual and organization needs to have the assurance that business conducted electronically is safely completed with the expected parties. This is not a serious problem when considering physical transactions because of the physical interaction of parties. However, things are way more complicated in a digital environment, since the available technology provides enough means for the monitoring, interception and forging of messages, as well as the impersonation of the participating parties. (Lopez, et al., 2005) As such, cases of corporate espionage, theft of intellectual property and E-commerce fraud, have become a great concern for most organizations. As an example, organizations involved in the international supply chain face such issues in their everyday operations. In this context, the role of trust management in information infrastructures is critical in order to address several issues of electronic security, particularly regarding the problem of secure identification of business partners. (Pruksasri, et al., 2012)

In relation to the research problem described in the previous section, it can be argued that organizations located in different countries face difficulties when it comes to exchanging data or resources, due to the absence of a universal trust model. In this sense, organizations have several challenges to overcome when trying to establish the identity of their transacting partners, as a common Point of Reference for both parties may not exist. Such issues are currently solved through cross certification processes, through the establishment of Bridge Certificate Authorities and through the mediation of web browsers. However, this is not always possible and, perhaps most importantly, a **global** trust network through the use of cross-certification or BCAs is technically infeasible to be established in the foreseeable future. In addition, we have also argued that embedding CA certificates in web-browsers is an inefficient solution. In other words, interoperability issues between *specific* trust domains might have been overcome, but this is done inefficiently and not on a global scale (Lopez Millan, et al., 2010) (Pala & Smith, 2010). At this point it must be stated again that this interoperability issues across different countries or regions is just one aspect of the general trust domains problem; nevertheless, it is used as it is a clear example of different domains.

1.2 The artifact

1.2.1 Description

So far we have argued that a universal trust model, one that can bridge the interoperability issues across different domains does not currently exist. In addition, (Daskapan, 2005) pointed out that as long as solutions are sought by relying on the same archetypes of trust models, a real breakthrough cannot be achieved, since all of them have particular shortcomings when it comes to a global scale implementation. In this aspect, the artifact to be designed in this thesis is a hybrid trust model, namely the "Trust Service Broker (TSB)", which will deal with trust as a derived service in order to facilitate resource sharing across different domains.

When end entities, for instance organizations, cannot agree on a common trusted Point of Reference, the Trust Service Broker can act as "*an intermediary by gathering multiple certificates from the local Certificate Authorities on the one hand and providing trust to end entities on the other hand*". A basic notion is that the TSB does not submit itself to any institution, as it respects the anarchistic principles of the internet. This is achieved as the TSB can be technically distributed as a service, even though it is logically centralized. In other words, *we could argue that it combines the best of both worlds, as it has credibility derived from multiple CAs and the flexibility of being nested as a peer* (Daskapan, et al., 2004). A high-level TSB model can be found in Appendix 1B.

1.2.2 Significance and implications

A crucial consideration for the design of the Trust Service Broker is that the issue of global distrust is not merely due to technical hindrances; also social and organizational issues are present, as demonstrated in Appendix 1A. This has two important implications. First, the problem is actually multidimensional and it must be dealt with accordingly. To put it differently, we cannot simply deal with the technical/infrastructural issues without accounting for other factors. In other words, *the organizational and national issues associated to the problem of global distrust define the "**boundaries**" in the design of the Trust Service Broker*. A high level overview of the most important stakeholders is provided in Appendix 1C. Second, the significance of a solution is also evident from a business perspective, since enabling global trust in information infrastructures can be a crucial step towards achieving trust on higher levels, thus facilitating the growth of e-commerce.

To elaborate more on that, the main focus of this thesis is to take **a specific business case in order both to specify the global distrust problem from a business perspective and also to apply the TSB architecture in this particular case**. The trust domains problem, as described in section 1.1.1, is a generic one. In the environment where the TSB solution will be applied, we will focus on the interoperability issues between organizations located in different countries. In this sense we will deal with a particular aspect of the general problem. More specifically, we will demonstrate how the TSB can be an efficient solution to the problem of information and resource exchange between different actors involved in the international supply chain. More specifically, we will deal with a logistics case scenario, with organizations involving an import trade lane from Malaysia to the Netherlands, where entities from different countries and supply chain communities are involved.

1.3 Research Objective and Questions

The significance of the online global distrust problem becomes more evident when considering the current globalization of the economy. For instance, it is clear that the business landscape is witnessing widespread migration of service functions from more developed nations, like the Netherlands and the US, to various foreign destinations, like India and China (Kedia & Lahiri, 2007). Since transactions on a global scale normally require the constant exchange of digital information in a secure way, the importance of the existence of an online global trust model is more evident than ever. In this aspect, the main **objective** of this research is to propose "***an alternative solution, namely the Trust Service Broker architecture, to enable secure and efficient information exchange between information infrastructures that reside across different geopolitical domains, independent from the consent of governmental organizations"***.

At this point it should be evident that our work builds further on the work of (Daskapan, et al., 2004), where a Trust Broker was first defined as a concept. To be more specific, our contribution is twofold; first, the TSB concept is refined and expanded to a detailed TSB architecture and second, the architecture is examined within the international supply chain environment, as a means to demonstrate its effectiveness in a specific context.

Since the main focus is on organizational activities, particularly in relation to the international supply chain, we are looking at a technical solution but within a particular business context. In this sense, the main **research question** becomes:

Q_0: ***"What are the components, communication processes, functions and internal security controls of the TSB architecture so that organizations within the international supply chain can efficiently exchange information and resources?"***

In order to answer the main question, the following sub-questions will be addressed throughout this paper as well:

Q_1: *"How is the trust domains problem related to the information flows between partners within the international supply chain?"*

Q_2: *"What are the design requirements for the TSB in the international supply chain case?"*

Q_3: *"What are the constituents of the TSB architecture in relation to the international supply chain case?"*

Q_4: *"Based on a risk assessment, which internal security risks can be identified regarding the TSB operations?"*

Q_5*: "To what extent can the TSB solution be validated and generalized?"*

1.4 Design approach / Methodology

1.4.1 Overview

This research will be primarily based on the Design Science Research Methodology (DSRM) principles, as presented by (Peffers, et al., 2008), with some adaptations and secondarily on the design research guidelines as proposed by (Hevner, et al., 2004). Figure 1.5 provides an overview of the phases related to the design of the Trust Service Broker.

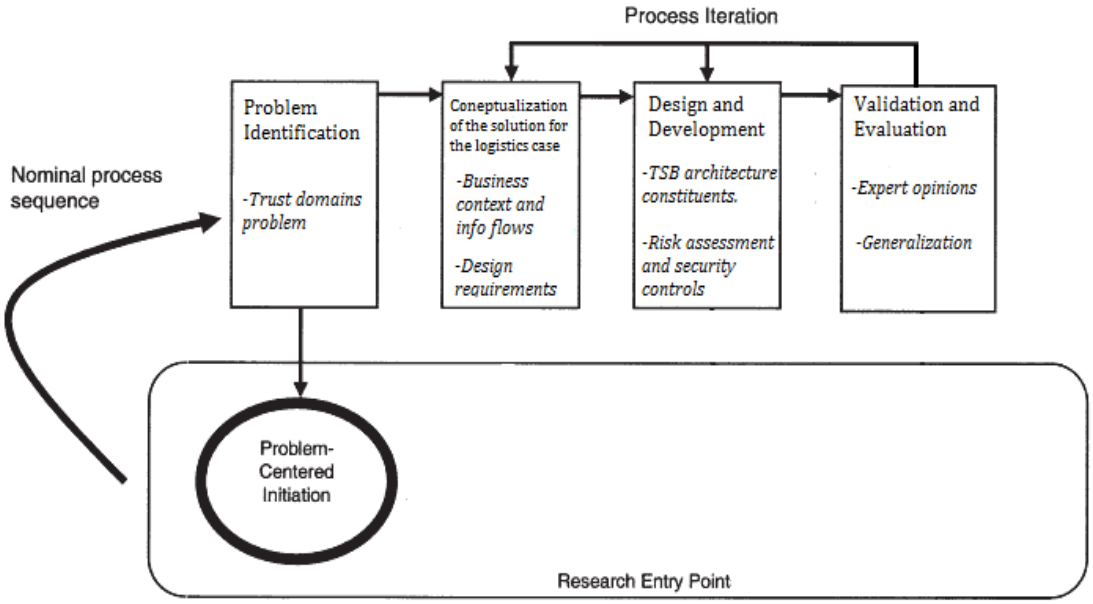

Figure1.5: DSRM process for the Trust Service Broker. Adapted from: (Peffers, et al., 2008).

In addition, the research guidelines proposed by (Hevner, et al., 2004) will be taken under consideration regarding the design of the TSB as a solution to the trust domains problem. For instance, according to (Hevner, et al., 2004), utilizing the available knowledge must produce an artifact (the TSB architecture in this case – Hevner et al guideline #1) which is relevant to the environment, i.e. people, organizations and technology. At the same time, it will have to add to the current knowledge base and be applicable in the appropriate environment: the international supply chain. These considerations are depicted in figure 1.6 and will be taken into account throughout all phases of the TSB design.

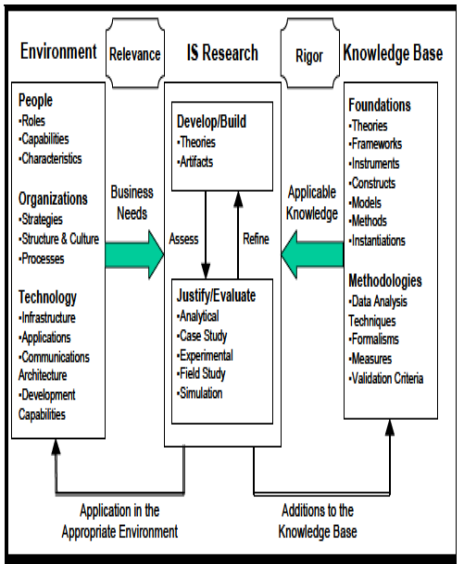

Figure 1.6: Information Systems Research Framework Source: (Hevner, et al., 2004)

1.4.2 Detailed design cycle

Problem Identification and Motivation

In design science, it is very important to first establish a deep understanding of the problem before actually considering a solution. In this first phase of the design process, we will further demonstrate the implications of the trust domains problem to the practical logistics case. To do so, the information flows between the main stakeholders involved will be described in further details in order to better demonstrate the business implications of the problem. As it is apparent, the first sub-question will be addressed during this phase.

At this point it should be further clarified that a **problem-centered approach** has been adopted. We have defined the research problem as follows: **"**There exists no universal trust model to efficiently provide a secure communications path across different trust domains worldwide**"**. In this sense, the need of developing an alternative trust model/architecture is triggered exactly by this problem. In addition, it is evident that this research addresses an important business problem in a unique way and can therefore be considered as a design-science research as defined by (Hevner, et al., 2004).

Conceptualization of the solution with regard to the logistics case

As already discussed, the objective of the TSB architecture with regard to the logistics case is to facilitate information and resource sharing among actors located in different trust domains. In this aspect, before we can consider the design of the architecture it is crucial to consider the major issues associated to the information flows between actors involved in the international supply chain. By doing so, the functional requirements for the design of the TSB architecture can be more accurately formulated and the solution will thus deal with the problem more efficiently. Therefore, in this phase the second sub-question will be addressed, in order to prepare the way for the design of the TSB architecture.

Design and Development

The third and fourth sub-questions are addressed in this phase, which is related to the actual design and development of the TSB architecture. This is done by taking into account the requirements that were previously established and it involves two main steps. In the first step the constituents of the TSB architecture are defined. This includes a high-level TSB conceptualization (for instance the TSB distributed concept), as well as a detailed description of the TSB architecture components and how they can be utilized in order to meet the design requirements. The second step involves a risk assessment in order to derive the necessary TSB security requirements and controls.

In this phase, the rigor of the research will be mainly derived from the effective use of prior research, such as practical problems, existing artifacts (eg. current trust models and risk assessment guides), Kernel Theories and analogies (Iivari, 2007) (Hevner, et al., 2004), all in relation with the international supply chain case scenario.

Validation and Evaluation

In this phase, the TSB solution is validated, which also involves getting the opinions of experts, thus addressing the fifth sub-question and satisfying Hevner's Guideline #2 (Hevner, et al., 2004). This will reflect on all phases of the design cycle in order to determine

that all aspects of the problem have been addressed and that the solution is in line with the requirements that have been set. Finally, in this phase conclusions will be also drawn, particularly concerning the generalization of the results and the implications for future research.

1.5 Thesis outline

Figure 1.7 provides an overview of the thesis, which follows the logical structure of the research questions, as well as the design phases.

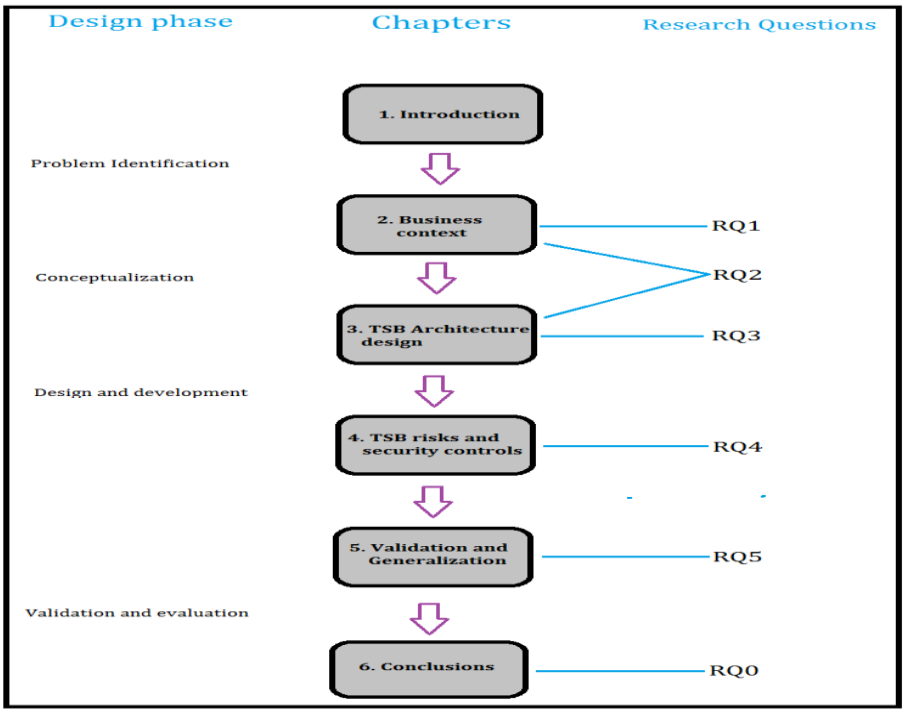

Figure 1.7: Thesis outline

Chapter 1 provides an introduction to the generic trust domains problem and the TSB solution on a broad level, as well as the adopted design approach. Chapter 2 refines the level of this thesis' focus to an aspect of the generic problem, specifically its implications on stakeholders involved in a practical logistics case. In this aspect, the specific case is described in details, along with the information flows and the practical considerations of the problem for organizations involved in the international supply chain, thus addressing the first sub-question. Based on these considerations, a first insight of the TSB requirements is presented, thereby addressing the second sub-question on a high level. Chapter 3 begins by further addressing the second sub-question and, in addition, the constituents of the TSB architecture are described in details, thus also addressing the third sub-question. Chapter 4 deals with the fourth sub-question by providing a detailed TSB risk assessment, along with the proposed internal security controls. Finally, the fifth sub-question is addressed in Chapter 5, which deals with the validation of the TSB solution for the logistics case under consideration. In addition, conclusions related to the main research question, remarks and implications for future research are also provided in this chapter.

CHAPTER 2: Business context

2.1 Overview of the international supply chain scenario

2.1.1 Introduction

This chapter provides an overview of the business processes, activities and stakeholders involved in a particular logistics case scenario, as well as an example of the information flow between involved actors. Appendix 2A gives a detailed description about the general context regarding the international supply chain and the role of information exchange. The interested reader can find arguments on the necessity for enhanced visibility of the supply chain, which is supported by ICT innovations, such as the data pipeline concept developed under the ongoing CASSANDRA project.

The benefits stemming from the use of novel IT solutions in the international supply chain are not gained without risk, since IT can remove protective barriers around assets and processes. To elaborate on that, greater levels of collaboration may expose more sensitive information to potential risk, thereby suggesting that emphasis must be placed on securing this information (Smith, et al., 2007). In addition, the dynamic scene in the international supply chain with numerous involved actors – sometimes with different or even conflicting interests – further commands the need for securing the information exchange. After all, all participants are known and should be considered trustworthy (Hulstijn, et al., 2012). This notion of trustworthiness should not only hold for the financial and transaction flows within the supply chain environment, but for the information flow as well. In this sense, we consider that the following logistics case is an ideal scenario in order to demonstrate the TSB effectiveness.

2.1.2 Case description

One of the key notions within the CASSANDRA project is the “Living Lab” approach, which was originally introduced in the ITAIDE project. (Tan, et al., 2011) defined Living Labs as “collaborative platforms for development and real-life testing of innovative IT-enabled solutions for international trade”. In this sense, actors from business and government cooperate in a real-life environment in order to develop and evaluate such ICT solutions. In addition, Living Labs as used in the CASSANDRA project aim to create an environment in which network collaboration and adoption of the solutions can successfully take place (Stijn, et al., 2011).

An example for such an environment for the CASSANDRA project is the Seacon Living Lab Asia-Europe. Seacon Logistics, a Dutch-based maritime logistics chain director, is a key actor in this Lining Lab and has identified three trade lanes which will be used for testing and evaluating innovative ICT solutions, such as the data pipeline. The first focus will be on trade lane 1, an import trade lane from Malaysia to the Netherlands and depending on the commitment of other stakeholders the other trade lanes will be added to the solution later (CASSANDRA, 29-04-2012). For the purposes of this Thesis, our efforts will also be focused in adapting this particular trade lane to a suitable logistics case scenario, in order to

demonstrate the effectiveness of the TSB architecture. A visual representation of the Seacon Trade lane 1 is given in figure 2.1.

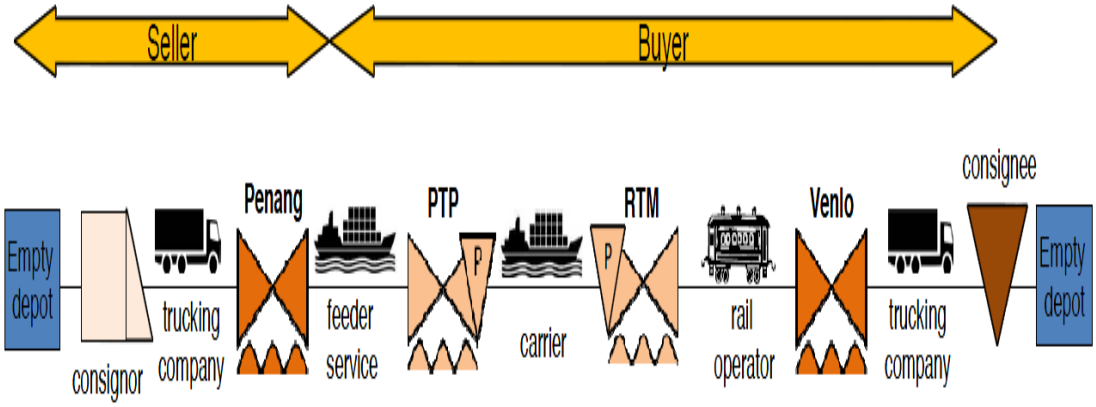

Figure 2.1: Seacon Trade lane 1, overview. Source: (CASSANDRA, 29-04-2012)

The consignor (seller) is a Malaysian company that provides spare parts for copier machines, located at Penang. The trade lane ends at the consignee located in Venlo, the Netherlands, with the focus is on direct FCL shipments. Seacon Logistics acts on behalf of the consignee, while its Malaysian partner, works for the consignor as freight forwarder for pre-carriage. The trade takes place under the Incoterm Free on Board (FOB), which suggests that responsibility for the goods and transport is transferred from consignor to consignee upon loading of the container on the ocean vessel (CASSANDRA, 29-04-2012).

We will first describe the processes related to the transportation of goods, as depicted in figure 2.1 presented above. The initial step is pre-carriage, consisting of a trucking leg and a feeder service, and takes place at the Malaysian side. The Malaysian Freight Forwarder arranges trucking from a local hauler and books feeder services between the ports of Penang and Tanjung Pelepas. Apart from the feeder service, the same company is also responsible for the deep sea leg, i.e. transportation from Penang to Rotterdam, and the booking arrangements are made by the Malaysian Freight Forwarder. Next, Seacon decides on behalf of the consignee about the on-carriage from Rotterdam to the consignee's warehouse in Venlo. The carriage between Rotterdam and Venlo is done through train or barge transport, with the same operator in both cases. Finally, Seacon arranges truck transport through local trucking companies for the final delivery of the goods to the consignee.

An overview of the involved actors, categorized in terms of the region of their operations, is presented in table 2.1.

MALAYSIA	THE NETHERLANDS
Consignor	**Consignee**
Freight Forwarder (Seacon's partner)	**Seacon**
Customs Broker	**Dutch Customs**
Malaysian Customs	**Port of Rotterdam**
Malaysian Ports	**Rail / Barge Operators**
Local Hauler	**Local Trucking companies**
Sea Carrier	

Table 2.1: Actors involved in the described trade lane

Table 2.1 includes the actors related to the supply-chain process. These actors range from intermediaries, authorities and ports to actors directly involved in the physical transport. As it is apparent, apart from the transportation of goods, the declaration of goods also requires the involvement of certain actors. More specifically, at the Malaysian side, information for export declaration is initially provided by the exporter (consignor). This information is then provided to the Malaysian Freight Forwarder who subsequently forwards it to the customs broker, who is in turn responsible for making the export declaration to the Malaysian customs. In this "chain" of information forwarding, the consignor is the party liable for the correctness of the declaration. Finally, on the Dutch side, the importer is fully responsible and reliable for the import declaration.

The series of processes related to the described trade lane are formalized and described more comprehensively in the following UML activity diagram, which was created by having in mind guidelines and proposed transformations (also involving the introduction of WAIT nodes at certain points) as presented by (Eshuis, 2006). Invocation (action) nodes are represented with the blue circled rectangles and object nodes with white rectangles. Decision/merge nodes are represented with the blue diamond shapes, while fork/join nodes with straight lines. The initial state is represented with a dot and the final states with a dot inside a circle. The broader defined areas indicate which actor is responsible for each activity.

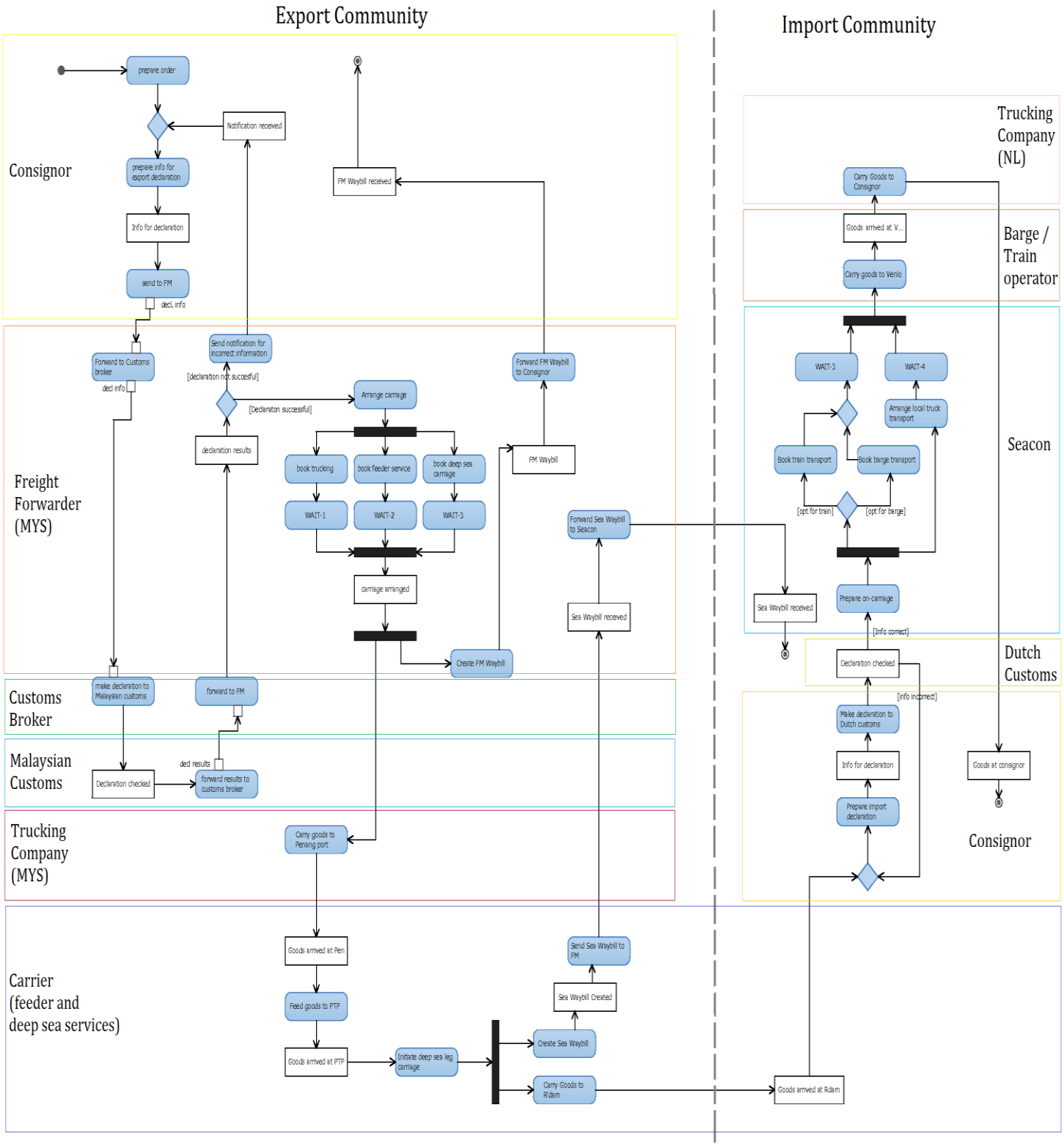

Figure 2.2: UML Activity diagram describing core business processes (activities).

An important assumption in this diagram is that potential issues with declaration of goods are associated with mistakes in information provision by responsible actors (consignor and consignee). In this sense, other causes for unsuccessful declaration (eg. mishandling of goods during transport or foul-play) are excluded and hence not represented in this diagram.

Before we present an overview of the information flow, it is important to make a distinction between the exchange of information which is directly related to the business activities regarding the movement of goods (as described in figure 2.2) and the one related to obtaining a view of the shipment process. To give an example of the exchange of information directly related to business processes, the link between the consignor's Information System and the Freight Forwarder is done using printed invoices and other information details (scanned and e-mailed), which are subsequently used to make the export declaration. Moreover, the Freight Forwarder uses an excel-based form in order to maintain shipment details and provide the consignor with a Waybill. However, apart from the information exchange which is necessary in order to arrange and facilitate the carriage of goods, it is also important for actors to be able to get an overview of relevant information for additional purposes. For instance, both the buyer and the seller would be interested to get a view of completed milestones. In addition, Dutch customs for example can get a more reliable overview of shipment details when all the information is available at a single point and originates from the source (rather than the information provided by the seller). This will be dealt with the introduction and configuration of the data pipeline developed in the CASSANDRA project. More details about the current state of actors' IT systems and the future state with the data pipeline configuration are available in appendix 2B.

2.2 Information flow between the entities

2.2.1 High-level overview

So far we have discussed that information exchange between actors can be directly related to the business activities (presented in figure 2.2), but also for tracking milestones and obtaining a view of the shipment process. A more formal high-level overview of the information flow can be provided through a logical Data Flow Diagram. Figure 2.3 provides an extensive logical DFD (i.e. not indicating technologies used, which processes or data stores are automated, or security measures), starting with the consignee placing the consignment order and ending by receiving the delivery order (with the goods).

In this figure it is apparent that on the export side, most of the relevant information is available through the Freight Forwarder. In this sense, an accessible data store (which can be provided by keying all the information in the FF data store) is essential in order to provide visibility for all partners, through GS1 or Seacon. In figure 2.3 all this information, along with shipment details at the export side, is captured and stored in Seacon's DB.

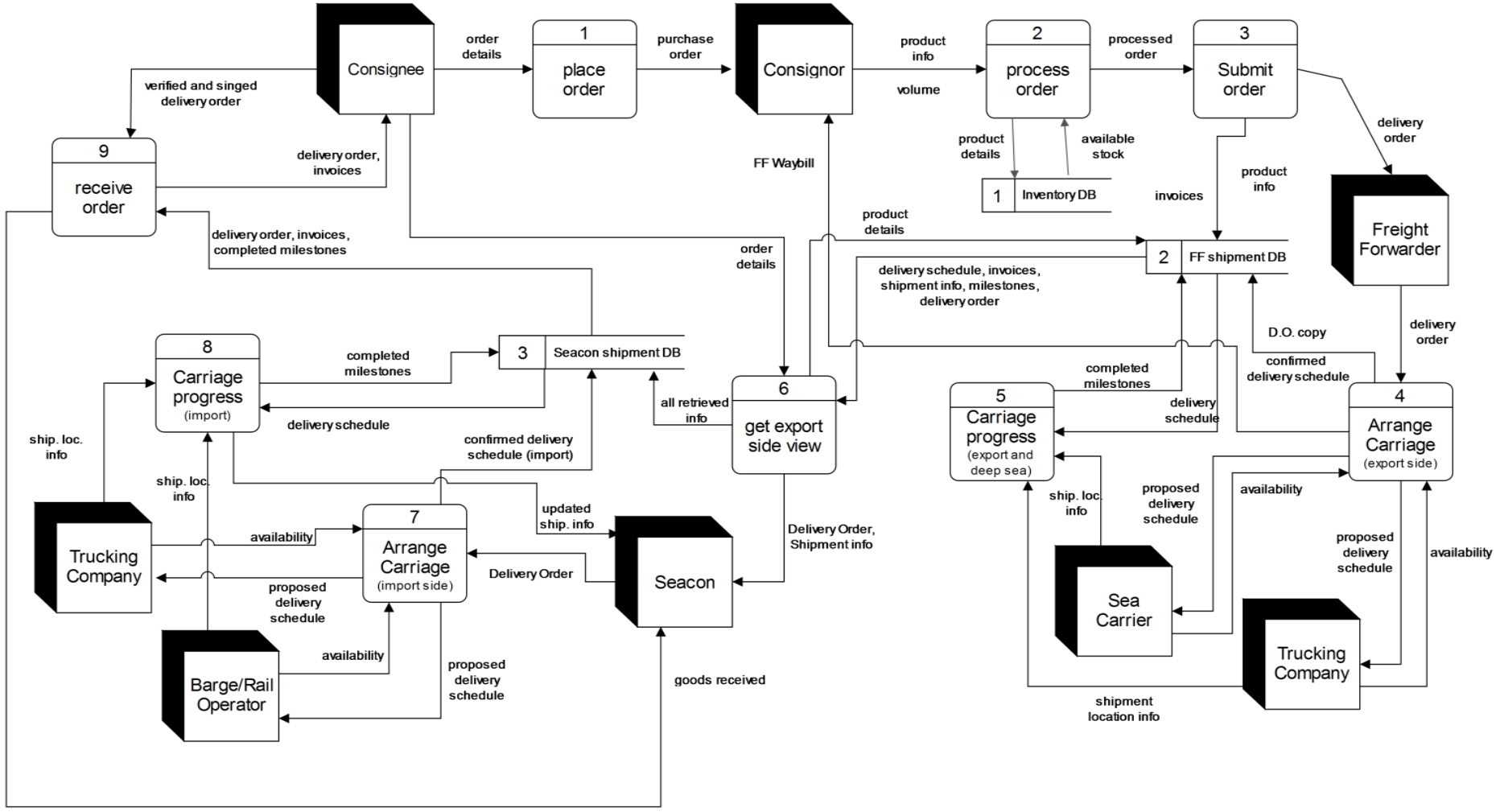

Figure 2.3: Data Flow Diagram (mostly related to business operations)

Two examples showing how the information can be used for visibility purposes by involved actors (eg. customs) are presented in figure 2.4. The first one involves the customs comparing the declaration information provided by the consignee with the information available in Seacon's database. The second example describes the data flow in the occasion where the consignee wishes to view the shipment progress.

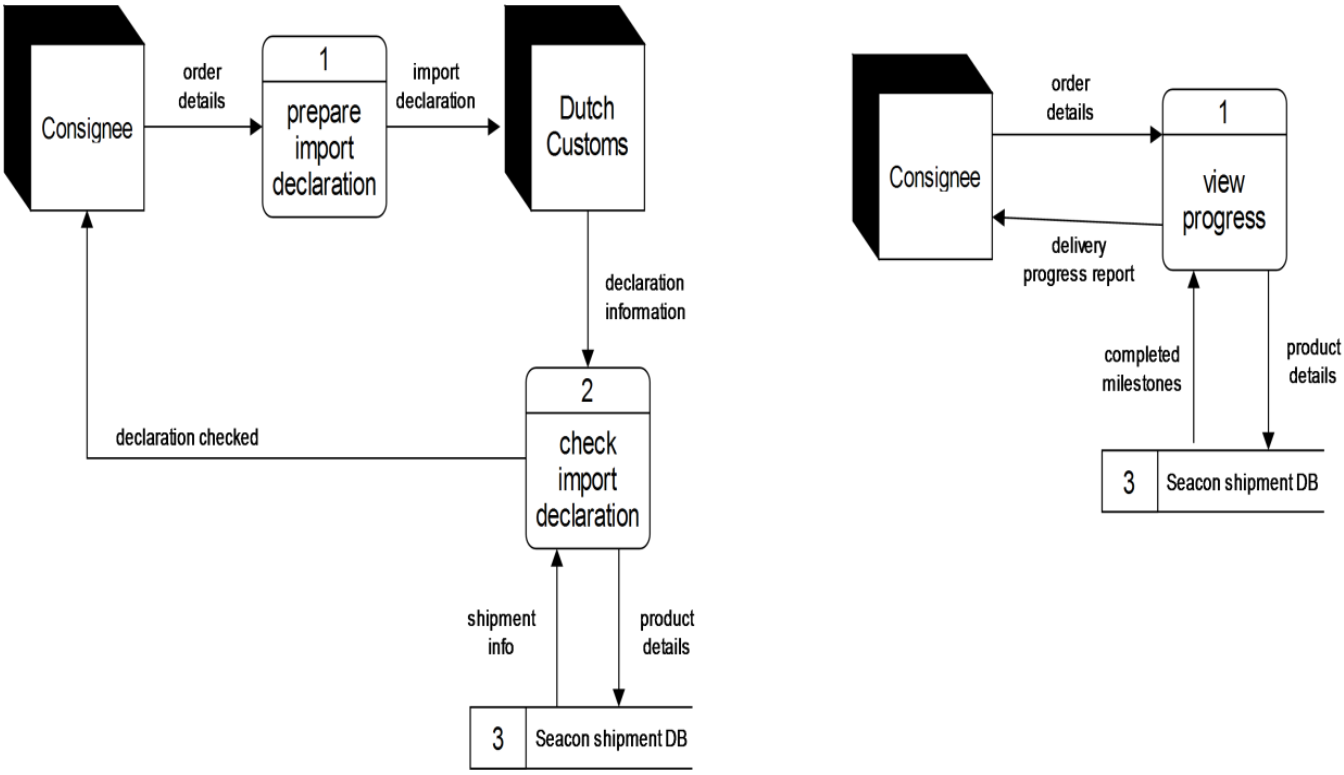

Figure 2.4 Examples of data flow for visibility purposes

It must be noted here that the above figures do not necessarily depict *all* information flows that may take place, but rather pose an example of the kind of information that is exchanged before, during and after the shipment of goods. For example, not only Seacon's databases hold all relevant information, but GS1 has also the same information available in order to provide a view for Malaysian parties (eg. customs and the consignor). Nevertheless, the corresponding data flow between the GS1 database and these actors is in essence similar to the ones described above and is thus not depicted. In any case, for the purposes of this Thesis, these DFDs are merely presented to demonstrate instances of data flow between the involved actors and the related business processes.

Finally, figure 2.5 presents a fictitious, yet representative, System Diagram in relation to the actors' information systems. The focus has been on the overall process of obtaining a view of the product and shipment information by actors in the import side.

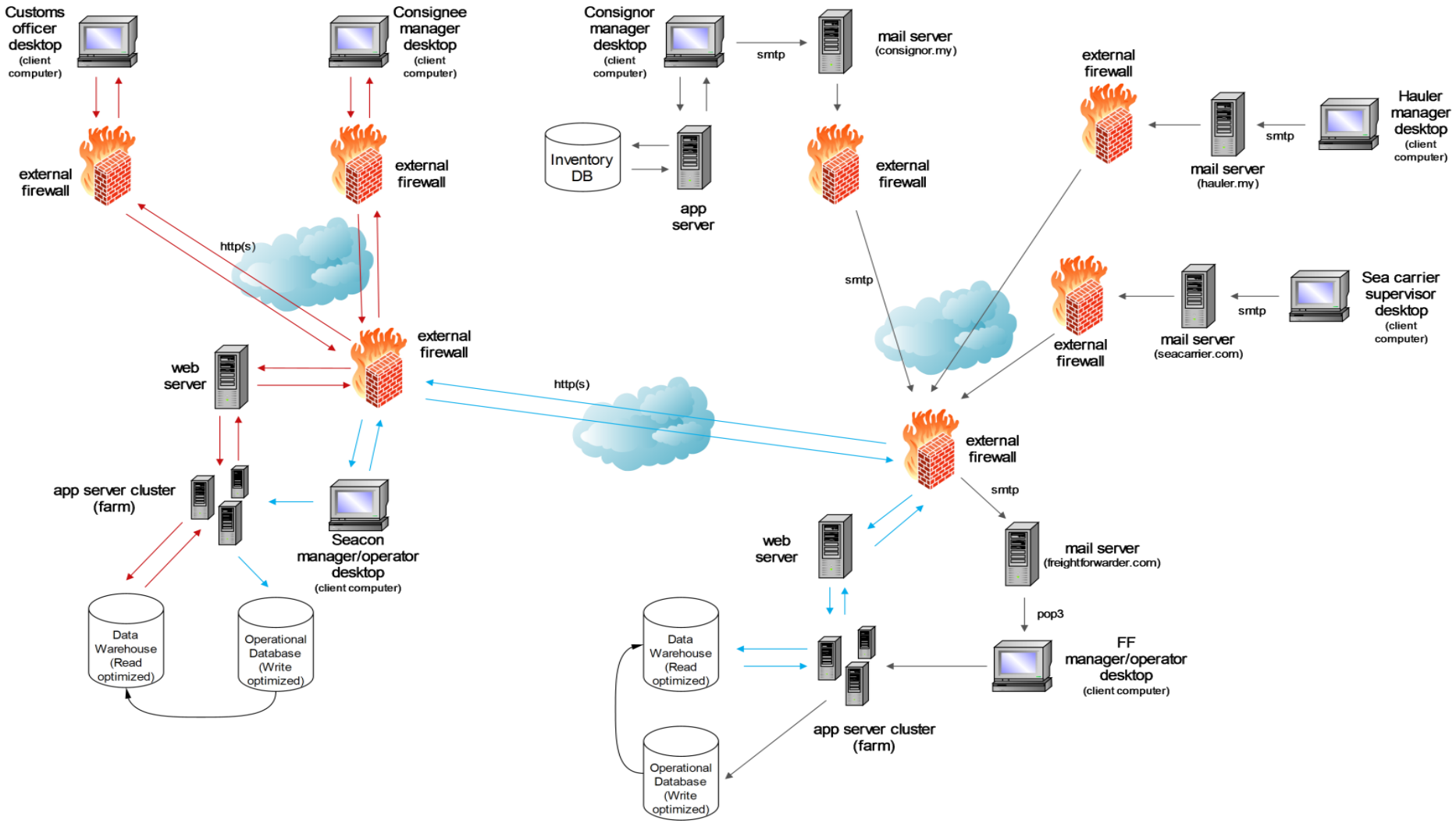

Figure 2.5: System Dynamics Diagram: obtaining an import-side view

It can be seen from this diagram that the process of obtaining an import-side view of product and shipment information consists of three sub-processes. First, all information on the export side is sent to the Malaysian freight forwarder (via e-mail). For instance, the consignor provides product information and the commercial invoices, while the local hauler and the feeder/sea carrier give information about shipment location. In addition, the freight forwarder has the task of converting the received information into a form that can be easily accessible by Seacon (by keying the information into the FF's database). Flows associated with this sub-process are depicted with grey arrows. Second, this information is stored in Seacon's database. The related flows are depicted with blue arrows. Third, Seacon provides, upon request, this information to interested parties, with an example being the consignee and the Dutch Customs (via the web). The relevant information flow is depicted with red arrows. This information can be also available to other parties, even at the import side, depending on the configuration. In addition, it must be noted that Seacon also holds information about shipment location on the import side, which is obtained by the local operators in a similar manner as on the export side, via e-mail (not depicted in this diagram for this reason). Finally, since both Seacon and the FF can be assumed to hold a significant amount of data, we have also depicted the separation of the operational database (write-optimized) from the data warehouse (read-optimized) and also the presence of server clusters (farms) for handling the load, both done in order to increase performance.

2.3 Deriving the design requirements

So far we have been dealing with a three layer approach for the supply chain management, making a distinction between the logistics, financial and information flows. The constant provision of correct and reliable information to customs and other authorities can prove invaluable for the smooth flow of goods by reducing both delivery times and administrative burdens (Xu, 2013). Even the smallest mistakes and disruptions in the information exchange between supply chain partners can be devastating in terms of lost revenue and goodwill (Deane, et al., 2009).

So the question now becomes: *What are the problems that may hinder the efficient and secure information exchange between supply chain partners?*

2.3.1 Establishing Global Identity

The first, and perhaps most prominent, issue relates to the establishment of the supply chain actors' identities. The challenge becomes even bigger when we consider a global environment. It is widely discussed in literature (Smith, et al., 2007) (Deane, et al., 2009) that the problem of *impersonation* is a thorn in the online business world and, subsequently, in the international supply chain operations. No matter how advanced cryptographic means are used for protecting the sensitive information, if a malicious external entity manages to successfully impersonate one or more of the supply chain partners, then severe disruptions and great financial losses are guaranteed as a result of the "leakage" of sensitive information. It is evident that lack of trust is the main issue towards establishing a secure global identity and, consequently, our efforts will be focused on this direction.

- ***ID verification***

To begin with, it is of paramount importance that a *trusted* identity of involved actors can be established, so that subsequent authentication of the origin of messages, as well as their integrity and confidentiality, can be ensured. In other words, trust is a critical enabler in order to achieve the ***verification of the identity*** of international supply chain partners. At this point it should be made clear that this issue merely relates to identity trust. Even if the identity of the actors can be verified, this does not mean that all actors can be entrusted with access to all information. To be more specific and in line with the described logistics case, only Seacon and the Malaysian Freight Forwarder should be able to have access to *all* available information, at least initially (CASSANDRA, 29-04-2012). Finally, supply chain operations can benefit vastly when certain actor ***capabilities*** can be verified, so that their partners can utilize them more efficiently. Although this is also an important concern and some potential solutions will be briefly presented in chapter 3, it is still outside of the main focus of this Thesis and therefore not examined in much detail.

- ***Unique naming***

The global distribution of the supply chain actors can pose additional concerns. In order to effectively verify the identity of each actor, it is evident that every actor must be defined by a **unique** name. Apparently, a global environment can complicate the issue of unique naming, since it is not unlikely that two or more actors may possess (or choose) local names that coincide. If something like this happens, it may result in severe troubles to the process of information exchange, since it may be the case that information will end up at the wrong actor. In order to arrive to an efficient unique naming convention, it is important to not only look through a computer systems perspective, where the uniqueness of the identifier is all that matters, but also through a user perspective, as people still prefer to use locally meaningful names. To be perfectly honest, the fact is that an accepted global naming convention to solve all these problems does not exist (Lopez, et al., 2005) and, as a result, getting to an appropriate and workable naming convention can be a real challenge.

- ***Dealing with different trust foundations***

Another set of problems also arise from the fact that actors in the international supply chain are located in countries all over the world. To be more specific, actors in the international supply chain will most probably be parts of different chains of trust; one actor may be nested in a certain local PKI, the second actor in another (unrelated) PKI, while yet a third actor may be nested in a peer trust model, such as PGP. It is evident, therefore, that all kinds of local trust schemes are involved. Approaches presented in literature that attempt to deal with trust issues, from generic service models – such as the common gateway model presented by (Chiu & Chen, 2005) and a trust model for web-based supply chain management described in (Sharifnia, et al., 2009) – to solutions specifically focused in securing the seamless integrated data pipeline (Pruksasri, et al., 2012), make a common assumption (either explicitly or implicitly): that a common point of reference (for example a trusted third party such as a CA) existed, or at least could be agreed upon. Although such an assumption may be realistic in some cases, it might not always hold when we consider a global environment, for the reasons described in section 1.1 and as a result the solutions might prove to be non-workable in practice. In addition to this concern, different kinds of certificates can be associated with the different trust foundations. The certificate format

does not only vary depending on the trust model (eg. PKI vs PGP certificates), but significant differences can be found within the same models. For instance PKIs are defined by different standards and recommendations; one PKI could make use of the X.509 certificate format while another may use the SPKI standards (Lopez, et al., 2005), while versions can also differ. As a consequence, the provision of trusted ID to actors within different trust foundations is not an easy task.

2.3.2 Policy and business control

It should be evident by now that the issues hindering the establishment of a trusted global identity are direct consequences of the global distrust problem (as defined in section 1.1) in relation to the international supply chain scene. Apart from that, however, the *implementation* of an architecture to provide solutions to these issues can raise additional concerns. The transition from defining a trust model or architecture to the actual implementation requires the establishment of an organization which will be responsible for ensuring that the previous issues are solved (i.e. trust is provided and actors can communicate securely). In this aspect, it is imperative that, above all, a **well-defined policy** must be set, so that the relying supply chain actors can be supported efficiently when it is required. In addition, in order to guarantee the efficient operation, adequate resources must be maintained at all times. Finally, organizational issues, as well as legal and regulatory concerns can pose additional challenges. However, such issues are outside of this thesis scope and as a consequence the will be briefly discussed in chapter 5.

2.3.3 Internal security

Last, but not least, the presence of such an organization implies that additional risks and **security concerns** will be present and, as a result, additional challenges will have to be overcome. Dealing with such security concerns is a critical task, which requires a thorough investigation of potential security risks before an attempt to provide any solutions. This process will be described in more details in chapter 4.

2.3.4 Overview of design requirements

Based on the issues that were raised in the previous sections, table 2.2 provides an overview of the requirements that the proposed TSB architecture will have to meet.

CATEGORY	REQUIREMENTS
FUNCTIONAL-TECHNICAL **Establishment of trusted global Identity**	ID Verification (and also capability verification)
	Unique Naming
	Deal with different trust foundations
ORGANIZATIONAL - LEGAL **Policy and business control**	Establish a well-defined policy
	Maintain sufficient resources
	Comply with trade / government regulations
SECURITY **Guarantee internal security**	Protect key TSB assets against loss of availability, integrity and confidentiality (and also authentication / authorization and non-repudiation)

Table 2.2: TSB Architecture requirements

2.4 Conclusion

In this chapter we have addressed the first sub-question, namely "How is the trust domains problem related to the information flows between partners within the international supply chain". The first course of action was to identify such information flows between the actors. In order to do so, we had to describe the main actors involved in a particular scenario and present the related business activities. Based on this analysis, we were able to describe the most important information flows, which were related both to core business processes and also to shipment and milestone tracking. Next, and since our main purpose was to discuss the effect of the generic trust domains problem to the secure and efficient information exchange between actors in the international supply chain, we limited our attention to the most relevant information flows. In this sense, we mostly focused on the overall process of obtaining a view of the product and shipment information by actors in the import side, since it involved information exchange between different regions. The most prominent implications of the trust domains problem were discussed, as the absence of a common point of reference (eg. a CA) between the two regions under consideration (the Netherlands and Malaysia) can take its toll on the secure information exchange, mainly due to the difficulties in guaranteeing the identity of the involved actors.

Based on the implications of the trust domains problem on the exchange of information between the international supply chain actors, we also attempted to define the main set of requirements of the TSB architecture so that it can effectively provide a solution to these problems. As such, we also provided an initial answer to the second sub-question, "What are the design requirements of the TSB architecture in the international supply chain case". We have argued that the most prominent requirement regards the provision of a trusted ID for all involved actors (which can be broken down to ID verification, the establishment of a unique naming convention and the ability to deal with different trust foundations) and that meeting this set of requirements is the primary purpose of this Thesis. Nevertheless, we have also discussed that in order to have a successful implementation of the TSB architecture, legal and organizational requirements, as well as requirements for the internal TSB security should be also dealt with.

CHAPTER 3: Designing the TSB

3.1 Detailed analysis of the design requirements

In the last section of the previous chapter, the most important issues related to the information exchange between the supply chain actors were discussed. These issues were directly related to the global distrust problem, as defined in section 1.1. Based on this discussion, we were able to identify the design requirements for the TSB architecture, which were divided in three categories. The first and most prominent set of requirements is related to the establishment of a trusted global identity. The second category is related to policy and business control, whereas the third refers to internal security requirements. In this section we will present a more structured and detailed overview of these requirements, while also briefly describing the approach which is going to be used in order to provide solutions. In the remaining of this chapter, a detailed overview of the TSB architecture will be described, as well as a detailed solution to the first – and most prominent – category of requirements (establishing a trusted global identity). Chapter 4 will address the internal security requirements in more details. Finally, although policy and organizational concerns are outside of this Thesis' main focus, they will still be discussed (albeit to a limited extent) in chapter 5.

3.1.1 Establishing a trusted global identity

It should be clear that establishing a trusted global identity for the international supply chain actors is the main requirement of the TSB architecture and, as such, the main focus of this Thesis. In more details, the TSB should be able to:

- **Provide ID verification.** The TSB has the responsibility to guarantee the secure identification of the supply chain actors. This requirement is twofold. First, the TSB should be able to securely identify actors willing to subscribe to its services. This part aims at ensuring that every actor to which a qualified TSB certificate is issued has been properly identified. Second, the TSB should be able to provide subscribed actors with the necessary credentials in order for them to be able to securely identify each other when they need to exchange resources and information. In this sense, the TSB should guarantee that entity authentication, as well as message authentication, integrity, confidentiality and non-repudiation are possible.
- **Verify actors' capabilities and attributes.** We have also argued that the secure identification of actors does not mean that all actors can be entrusted with access to all information, while at the same time some actors may possess certain capabilities of importance to their partners and the possession of such capabilities may also need to be guaranteed. Although not the main focus of our research, this requirement can be met by using specific certificate extensions and, additionally, by issuing attribute certificates, as defined in (rfc5755, 2010).
- **Adopt a unique naming convention.** Since the TSB is meant to be deployed globally, an appropriate name convention for the relying entities must be defined and maintained. In this sense, it must be ensured that the TSB adopts a global name convention that can **support the unique naming of *all* actors in a *uniform***

manner. To guarantee the uniqueness of an entity's ID, which is crucial for the TSB system itself, the public key (more precisely its hash value) of the user can be used as a global ID, since it is a globally unique byte string, while also uniquely bound to a particular key holder. In order to also retain a degree of local meaningfulness, the hash string should be accompanied by a meaningful local identifier. For example the unique ID of a newly registered Seacon entity will be of the form: **GlobalName = (Kx, Seacon operations, local name-eg. Bob-)**, where Kx is the hash function of the entity's unique public key. By this, the name is globally unique (due to the key string), while also locally meaningful. In addition, we suggest that the "*Subject Alternative Name*" (SAI) extension should always be used to include local e-IDs or e-mail addresses when they exist in order to further promote reliability and facilitate the meaningfulness of the name. Furthermore, we must make clear that another purpose of the unique naming is to facilitate the search of partner certificates. A combination with the information included in the Authority Information Access (AIA) certificate extension (which contains an URI to point to the location of a particular certificate) can facilitate access to partner certificates. This can be done through several different protocols (eg. http, ftp or ldap). Finally, it must be also the case that certificates will be made publicly available for retrieval (by the TSB community) *only in those cases for which the certificate-holder has given its consent.*

- **Deal with different trust foundations.** The TSB architecture serves in order to interconnect actors nested in different trust domains. This means that the focus is not only to resolve interoperability issues between actors who are parts of PKIs in different countries, but also between actors nested in different trust models (both in the same and in different countries) for instance PKI to PGP. A straightforward implication of the different trust models is that the TSB should be also able to deal with all types of local certificates. In this sense, it must be able to validate certificates issued in different formats. We will provide further details on how the TSB is able to do so in the section 3.2, where we discuss about the TSB distributed concept. Finally, recognizing different types of certificates that the actors may already possess, since they are part of different trust domains, is only one part. After the registration to the TSB services, all actors are a part of the "TSB chain of trust". In this aspect, all certificates issued to actors should be under the same format. Given the business context of the TSB architecture and enterprise requirements, we propose that the certificates should be issued according to the (generic) X.509 v3 format, and that appropriate extensions depending on the circumstances are used.

3.1.2 Policy / Business control

The aforementioned requirements are crucial for successfully setting the scene of the TSB architecture. However, to guarantee a successful implementation, the TSB should also:

- **Establish a well-defined policy.** This is a crucial requirement of any PKI certification authority and such it should be a priority for the TSB as well. Before the registration

of an actor seeking to support his electronic signature via the TSB certification takes place, the TSB must inform the actor "*by a durable means of communication of the precise terms and conditions regarding the use of the TSB certificate, including any limitations on its use and defining the procedures for complaints and dispute settlement*" (Adams & Lloyd, 2002). This information must be also available on request to third-parties relying on this certificate.

- **Maintain sufficient resources to support relying entities when requested.** In the case of a dispute, the TSB should be able to assist in resolving the matter by providing relying evidence in a timely manner. In this sense, support (not limited to this example) should be provided by the TSB in case it is requested by an actor, in real time. In order to do so, the TSB must possess sufficient resources, in terms of infrastructure and personnel (particularly regarding competence at a managerial level). In addition, sufficient financial resources should be maintained in order to bear liability for potential damages (Adams & Lloyd, 2002)
- **Comply with regulations.** Finally, as an organization that provides its services to other parties, the TSB must also take into account additional organizational and legal requirements in order to consider a viable future implementation.

It should be made clear that these considerations are outside of our primary focus. Their significance, nevertheless, for a successful TSB implementation cannot be completely ignored and, as a result, some key considerations as well as the need for further research are discussed in chapter 5.

3.1.3 Internal Security

While the TSB architecture aims at securing the information exchange between supply chain partners through the provision of a trusted ID, it is also crucial that the TSB system itself must be secure. In this sense, requirements for the internal TSB security are also essential to be met so that the TSB system can operate smoothly and efficiently. Chapter 4 will deal with risks associated with the TSB system and the corresponding security requirements and controls in order to deal with them.

3.2 The TSB as a distributed concept

The purpose of the TSB architecture is to provide trust to the actors involved in the information exchange within a supply chain, as described in the case scenario. The TSB does so by providing registered actors with digital certificates, similarly to a PKI. The main difference, however, is that the TSB is not institutionalized like CAs, as it was discussed in chapter 1.

It should be clarified that the main offering of the TSB architecture is that trust can be provided to actors across different regions globally. The implication on the TSB from an organizational perspective is that it is not a single organizational entity, but rather consists of "hubs" distributed in every country throughout the globe. There are several reasons that make such an approach necessary. First, it may prove to be impossible for one TSB organizational entity located in a single country to gather certificates from CAs located all around the world, due to political and practical considerations. On the contrary, it is much

easier for each TSB hub to limit its focus on gathering certificates only from a local CA – or more CAs if different PKI domains exist within the same country – and also become a part of the local web of trust. Second, since the TSB is responsible for registering actors dispersed worldwide, the existence of many TSB hubs disseminated around the globe can greatly facilitate maintaining contacts and supporting these actors (Lioy, et al., 2006). Finally, a single TSB entity can be regarded as a single point of attack for external threats; a distributed TSB system on the other hand can offer additional reliability in this context.

We have argued that the TSB is able to provide trust to supply chain partners, without being involved in a chain of hierarchy. So the main question now becomes: how does the TSB guarantee its own trustworthiness? In other words, **how does the TSB got its authority and power?** Anyone could actually provide trust to other entities by granting his own certificates, as in the PGP model, but this does not necessarily mean that he can be considered trustworthy (Adams & Lloyd, 2002). In this aspect, it is important to first discuss how the different actors can actually trust the TSB itself.

To address this question we must again make the distinction between the online and offline environments. In the online world, the TSB derives its own trustworthiness by gathering multiple certificates from different local CAs. More specifically, each TSB hub is responsible for obtaining certification(s) from CAs residing in the same country, as already described. In this sense, actors located in different countries can trust the TSB system in general, because each one recognizes a particular certificate that was granted to the TSB (to a particular TSB hub to be precise) by a CA nested in the same domain as the corresponding actor. Therefore, the TSB model has the credibility of a PKI, but without drowning in the legal and administrative burdens associated with CAs, since the TSB hubs are nested as peers (Daskapan, et al., 2004).

To make things more clear, we must stress three distinct points. First, the TSB hubs can be regarded as "**trust anchors**" in a given local territory. Second, these hubs are not independent, but are **interconnected** both from an organizational (much like multinational firms) and from a trust model perspective (for instance through cross-certification means, as discussed in ch.4). It is precisely through these interrelations and organizational coordination that the TSB is able to gain its power and authority *globally*. Third, it is not imperative that a TSB hub should be anchored in every country; for several reasons this may not be possible – or even desired – due to increased complexity. In this sense, a particular TSB hub can obtain certificates from more than one country (mostly depending on proximity) and therefore act as a trust anchor in a broader territory. An illustration of the distributed TSB concept is presented in figure 3.1. To keep things simple, this figure includes 2 TSB hubs, one in NL and the other in MYS. In accordance to the third point, we assume (arbitrarily and merely for the purposes of illustration) that the Malaysian hub is also certified from a CA in Singapore. Another assumption is that both entities are part of the corresponding local PKI trust chains.

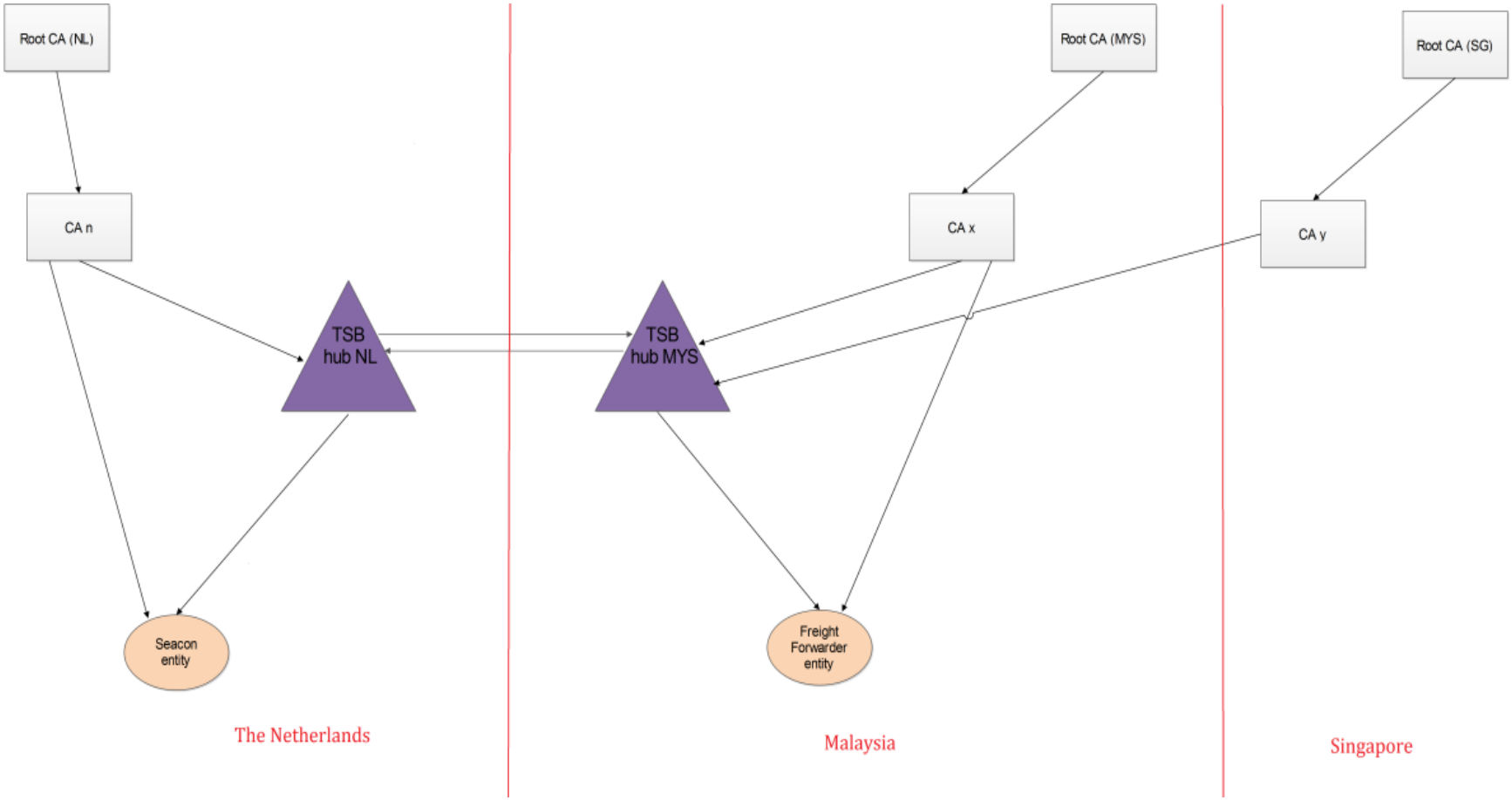

Figure 3.1: Distributed TSB concept and the chains of trust

Furthermore, equally important to establishing the online credibility of the TSB is also its trustworthiness when it comes to the real world. To be more specific, actors will want to be sure that the TSB will indeed deliver the expected services before they actually register. This is directly related to the second set of requirements, regarding policy, organizational and legal considerations. Although the implementation of the TSB is out of our scope, some thoughts and recommendations on these issues will be presented in chapter 5, also in an attempt to set the direction for future research.

To sum up, the TSB's main goal is to facilitate secure and efficient ***inter-organizational*** exchange of information. Figure 3.2 shows the place of the designed system (the TSB) in relation to the (simplified) network of actors which was more extensively presented in chapter 2. The focus is on the exchange of information between the consignor and the FF (via e-mail) and between Seacon and the FF (via the web) as will be described in more details in section 3.4. In this case, two TSB hubs are involved.

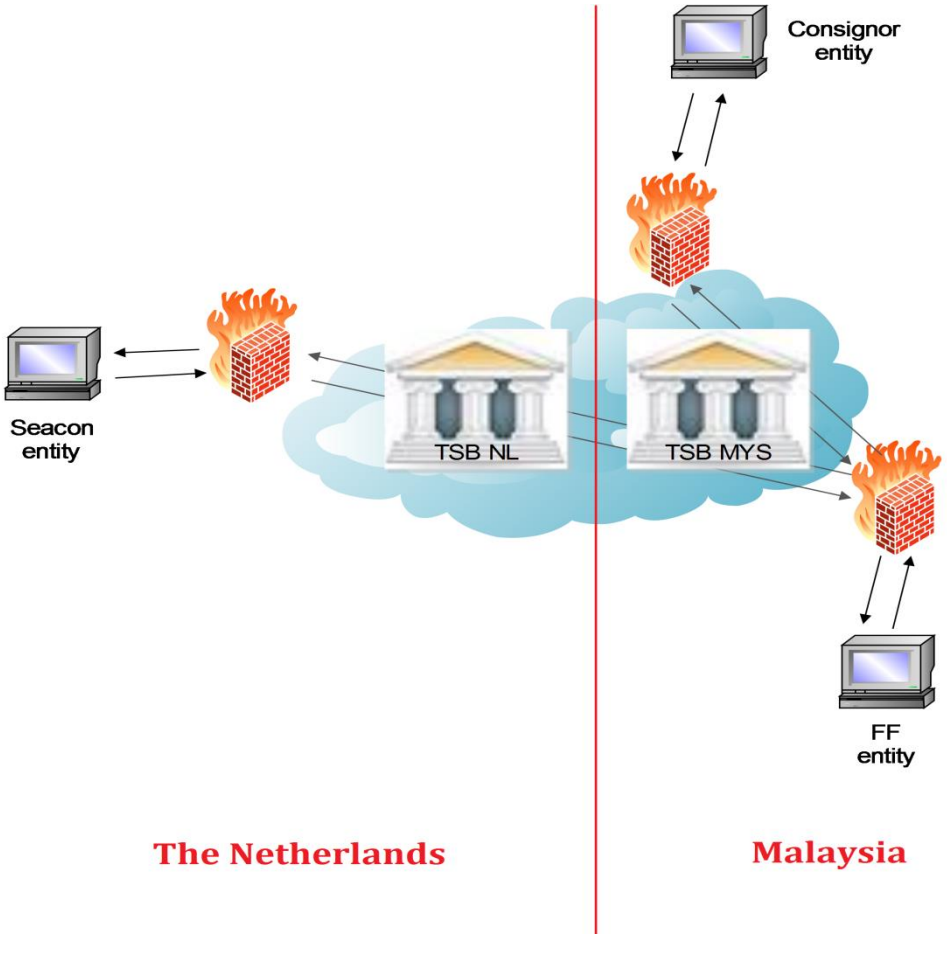

Figure 3.2: Indicative places of the system to be designed (TSB)

3.3 Components of the TSB architecture

In this section, we will take a closer look at the TSB architecture and its components. Figure 3.3, presented below, provides a detailed overview of the TSB architecture, consisting of four distinct layers of components. In addition, it should be clear by now that the TSB architecture also depends on existing trust chains (eg. local PKIs) and their components, which is also shown is the figure.

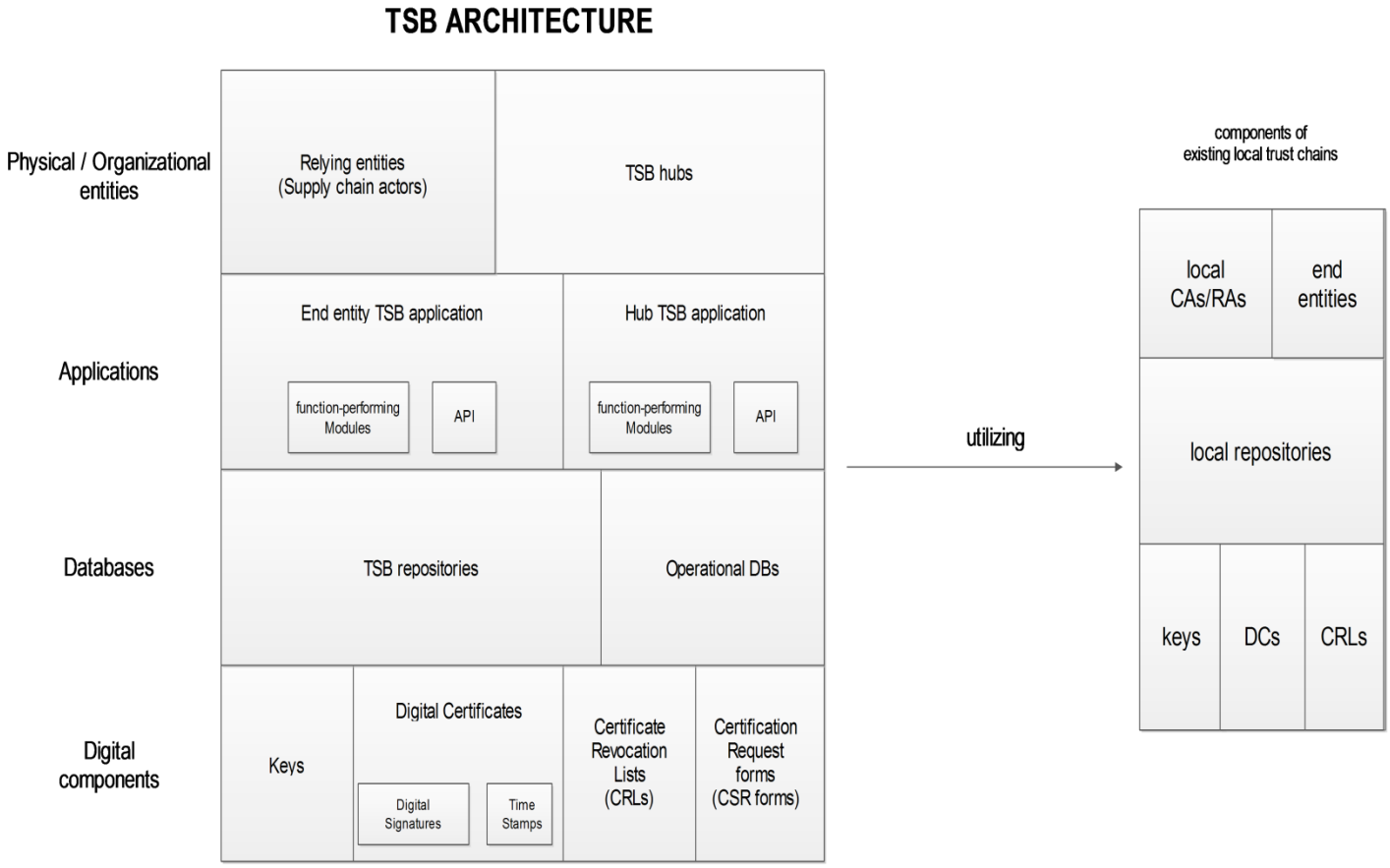

Figure 3.3: TSB architecture and its components

In the bottom layer are the **digital components,** which form the core of the TSB architecture. **Databases** which are used for storing and accessing the digital components comprise the third layer, while **enabling applications** form the layer above. Finally, on the top layer are the **physical/organizational entities,** namely the relying entities (supply chain actors) and the TSB hubs which assume various roles and responsibilities. To show the connection between the components in the different layers, we can say that "**the TSB architecture** ***consists of Digital components which can be stored in Databases and are accessed through enabling applications by the entities***". As an example, public keys and digital certificates are stored in the TSB repository (database) and can be retrieved by other relying entities through their applications in order to initiate a secure exchange of information. Another example involves storing the information contained in a certification request (CSR) form in the operational TSB databases by an application of the corresponding TSB hub, for registration and certification purposes. When an actor is already a part of an existing trust chain, digital components stored in local databases (eg. local PKI repositories)

are also utilized to facilitate processes such as TSB certification. This is a result of the fact that a relying entity within the TSB architecture may also assume the role of an end entity within a local chain of trust, which is also the case for the TSB hubs. The way the components of the TSB architecture (as well as external components when necessary) are used in order to meet the design requirements as presented in section 3.1 is described in section 3.4. We will now provide more details on these components.

3.3.1 Digital certificates

The main purpose of the TSB digital certificates is to guarantee the unique binding of a public key (and consequently the corresponding private key) to a particular relying party. There are various types of certificate formats, for instance X.509 public-key certificates, SPKI certificates and PGP certificates. Although PGP certificates enjoy a significant amount of use over the Internet, it does not make a good candidate a use within the TSB context, mainly because all trust decisions rest with individual entities and therefore suffer from reduced reliability. On the contrary, X.509 public key certificates are the preferred choice for these purposes. In particular, version 3 public-key certificates are the most flexible and many of their extensions are specifically targeted to support enterprise requirements (Adams & Lloyd, 2002). Among other things, they are also the main choice for supporting the exchange of e-mails composed in a MIME format, which is relevant to our case, as it is going to be described in section 3.5. For these reasons, we propose that the certificates issued by the TSB should be in a X.509 version 3 format. Figure 3.4 provides an overview of the fields included in version 3 public key certificates (El-Ashqar, et al., 2012).

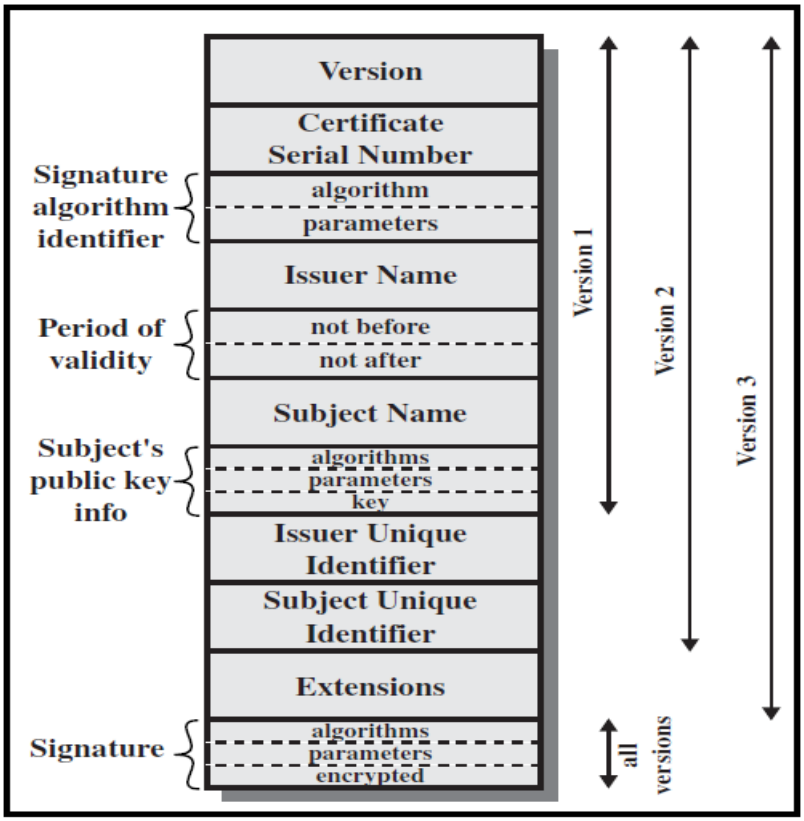

Figure 3.4: Public-key certificate formats. Source: (El-Ashqar, et al., 2012)

Extensions appear only in version 3 certificates. Some of the most relevant for the TSB architecture are: *Subject alternative name* (i.e. alternative name forms associated to the owner, such as e-mail or IP addresses), *Private Key usage period* (indicating the time window that the public key can be used to verify digital signatures after the corresponding private key has expired), *Authority Information Access (*for efficient access across the TSB repositories*), Subject Capabilities* and *Authority / Subject Key Identifier* (AKI/SKI). We have discussed that each subject may hold more than one key pairs for different purposes; the key identifier extension distinguishes between such multiple key pairs held by the same owner. The same can be applied for the certificates held by the TSB itself, since it holds certificates (and hence key pairs) from multiple CAs.

Finally, we have discussed that the TSB may also provide *attribute certificates* for access control purposes. Attribute certificates are not public key certificates; they are rather designed to convey attributes about a given subject. The attribute certificate may point to a public-key certificate in order to authenticate the identity of the attribute certificate holder (Lopez, et al., 2005).

3.3.2 Keys

As discussed, the TSB architecture is based on the principles of public key cryptography. In this sense, techniques used for encryption as well as for digital signatures involve a private and a public key. At this point we should also note that symmetric (secret) keys are also used when it comes to message encryption, since the symmetric encryption and decryption processes are much faster and more efficient. The public / private keys are therefore used to encrypt / decrypt the secret key that was used to encrypt the message (Schneier, 1996), as it will be shown in more detail in section 3.4.

Public / private key pairs can be generated through different mathematical algorithms, such as RSA (suitable for encryption/decryption, for signing/verification and key transfer) and DSA (designed exclusively for signing/verification). These are examples of algorithms that can be used by TSB entities for key generation, depending on their preferences and intended use; as we have discussed, according to the (rfc4210, 2005) specifications, entities should be able to use whichever algorithm they consider most suitable for their needs. Finally, the key length depends mostly on cost / benefit (message value) considerations (Schneier, 1996); however, as an indicator, the state of research suggests that both RSA and DSA keys should be at least 1024 bits long to provide adequate security.

3.3.3 Digital signatures and time-stamps

Employing a digital signature is the most common means to guarantee a message's authenticity and integrity. It involves the calculation of a message's hash value, for instance with an algorithm such as SH-1, and then "signing" this value with a private key, which can be generated through one of the aforementioned algorithms, for example DSA. By doing so, the recipient of a message can verify the origin (authenticity) of the message by using the sender's public key and then comparing the hash value appended on the message with the one calculated by himself. In case of a match, the integrity of the message is also guaranteed

(Choudhury, et al., 2002). A more comprehensive overview of the processes of creating and verifying digital signatures is presented in the e-mail scenario in section 3.4.

In addition, digital signatures are crucial in order to ensure non-repudiation, as already discussed. This usually also requires a time-stamping service. A time-stamp is created by the TSB by concatenating the date and time it received a message's hash value by the sender onto the hash and then digitally signing the result, which is described more extensively in appendix 3A. By this, the sender (recipient) cannot deny originating (receiving) a particular message created at a certain point in time.

3.3.4 Certificate Revocation Lists (CRLs)

The need to revoke an issued certificate may be a result of different circumstances, such as suspected private key compromise, or an entity's request to unsubscribe from the TSB's services. Initiation of a certificate revocation may come from the user (if for some reason he suspects that his private key has been compromised), or the TSB itself when deemed necessary. The most common method of providing information about certificate revocation is through the use of Certificate Revocation Lists. These lists can be directly retrieved from the TSB repository, in a similar manner as digital certificates. Figure 3.5 provides an overview of the base CRL fields according to the X.509 standards.

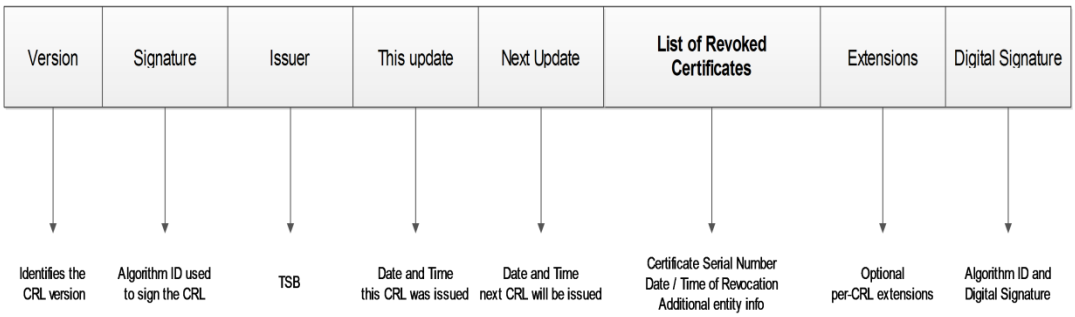

Figure 3.5: CRL fields

Nevertheless, the complexity and frequent inefficiency associated to using CRLs has been pointed out by many researchers (Gutmann, 2002). As a result, the TSB can additionally (or alternatively) offer an online status query function in order for end entities to quickly determine whether a particular certificate is still valid or not, in order to achieve even greater efficiency (Pala & Smith, 2010).

3.3.5 Certification request (CSR) forms

For the purposes of the public key certification process, subscribing actors must forward all relevant details to the corresponding TSB hub. In most PKIs, this is usually done through certificate request forms (Choudhury, et al., 2002). As it is shown in the initialization protocol in the next section, after the identities of both the actor and the TSB have been established, the actor generates his key pair and forwards the public key to the TSB hub for certification. The public key is officially provided via a certificate request form. Additional information may be provided by the actor (eg. details for alternative naming etc), but it is up to the TSB hub's administrator to decide which information will be kept and used. In

essence, the only necessity is to include the public key. These forms can be held in a **Pending Queue**, if approval cannot be done immediately (SQA, 2009).

3.3.6 TSB databases

The TSB architecture needs the prompt operation of databases which are used to store, archive and maintain several types of data. To be more specific, by this term we refer to:

- **Databases (repositories) for use by TSB subjects**.
- **Operational databases, used by the TSB system itself.**

Repositories can be regarded as "certificate libraries", meaning that they serve as a centralized store of the certificates that the TSB issues or revokes (Qing-hai, 2012). These Databases enable the retrieval of certificates issued to other entities. As described in section 3.4, each hub manages its own repository. Each database (repository) maintains:

i. The Digital Certificates of all subscribed actors *within the same region.*
ii. Additional actor information associated with each DC, in order to facilitate search and retrieval.
iii. Information about the status of these certificates (in the form of a Certificate Revocation List)
iv. The unique names of actors subscribed in other regions, along with information of where (which hub's repository) their certificates are stored and are available for retrieval. This information (matching the entry in the AIA extension field of the certificate) is used as a "pointer" to another TSB hub repository, in order to facilitate the retrieval of certificates of actors residing in other regions. This process is explained in details in section 3.4.

Databases only accessible to the TSB system itself maintain a collection of data critical for various functions of the TSB system. They can range from registration DBs (holding specific registration and other details about the registered entities) to functional DBs (maintaining archived documents, data related to system recovery needs, keeping audit logs etc.).

3.3.7 TSB application

It is apparent that the described components are utilized by a TSB application so that certain functions can be performed. This applies both to the TSB hub related functions, as well as functions performed by the relying entities.

With regard to the entities, the TSB application must be in place in the entity system so that the services of the TSB architecture can be delivered. In this sense, an application specifically designed to support the TSB architecture should be installed both in the hubs' systems and in the actors' systems upon successful registration. The TSB application therefore comes in two different "versions" (one for the hubs and another for the actors), with different modules, as different functions need to be performed. Figure 3.6 presents an overview of the TSB application architecture on a high-level, focusing on the most important modules and functions.

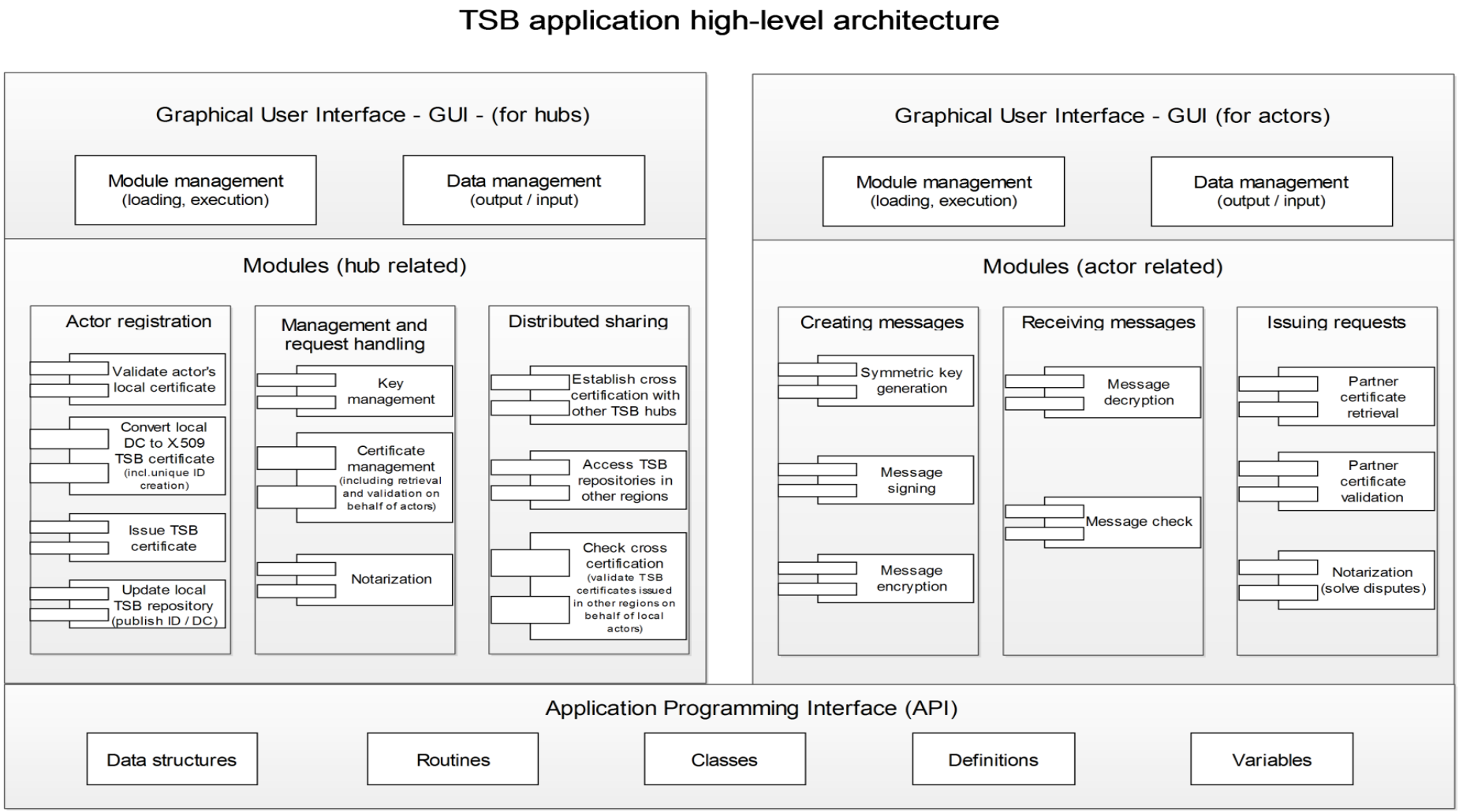

Figure 3.6: High level TSB application architecture

The distinction we have made between the hub and actor "versions" of the TSB application comes naturally, since they perform different functions which are therefore organized in different modules. Consequently, the Graphic User Interface also differs between the two versions (while we could also argue that the actor GUI should be more user-friendly as well). Nevertheless, the Application Programming Interface is common and can be regarded as a library containing elements (such as classes and definitions) which can be called during the execution of specific modules in both cases. Finally, further details on some of the most important functions will be provided in section 3.4, where we present the TSB initialization protocol and an example of message exchange.

3.4 Deploying the TSB: Initialization and cases of information exchange

Now that we have presented the design requirements, services and components of the TSB architecture, it is time to describe how the TSB can be deployed in order to facilitate secure resource and information exchange for the supply chain partners involved in the international supply chain case.

3.4.1 Initialization protocol

Perhaps the most important process with regard to an efficient TSB architecture is the initialization process, since it is essential in order for the TSB to be able to effectively perform subsequent functions. It involves the secure identification of relevant supply chain actors, their registration and TSB certification. In section 3.2 we have described the distributed TSB concept, which consists of organizational hubs nested in every country. Also, we have described in figure 3.1 that the TSB has the power to validate credentials, since each hub is certified by a local CA, while also being a part of the local web of trust.

The protocol presented in figure 3.7 illustrates a case of the initialization procedure. The Seacon entity is assumed to be already a part of a local PKI, having a DC issued by a local CA and a local ID, which also applies for the corresponding TSB hub. A different illustration of the registration of two actors in different domains (additionally showing the trust chains), is presented in appendix 3B. Finally, when a subscribing actor is nested in a PGP web of trust, the corresponding TSB hub can also validate the actor's identity (and vice versa) through the referencing mechanism inherent in the PGP model (by determining the level of trustworthiness that can be placed upon this actor). In this aspect, the actor's PGP certificate is "converted" to a TSB certificate in a similar manner as in the case shown below.

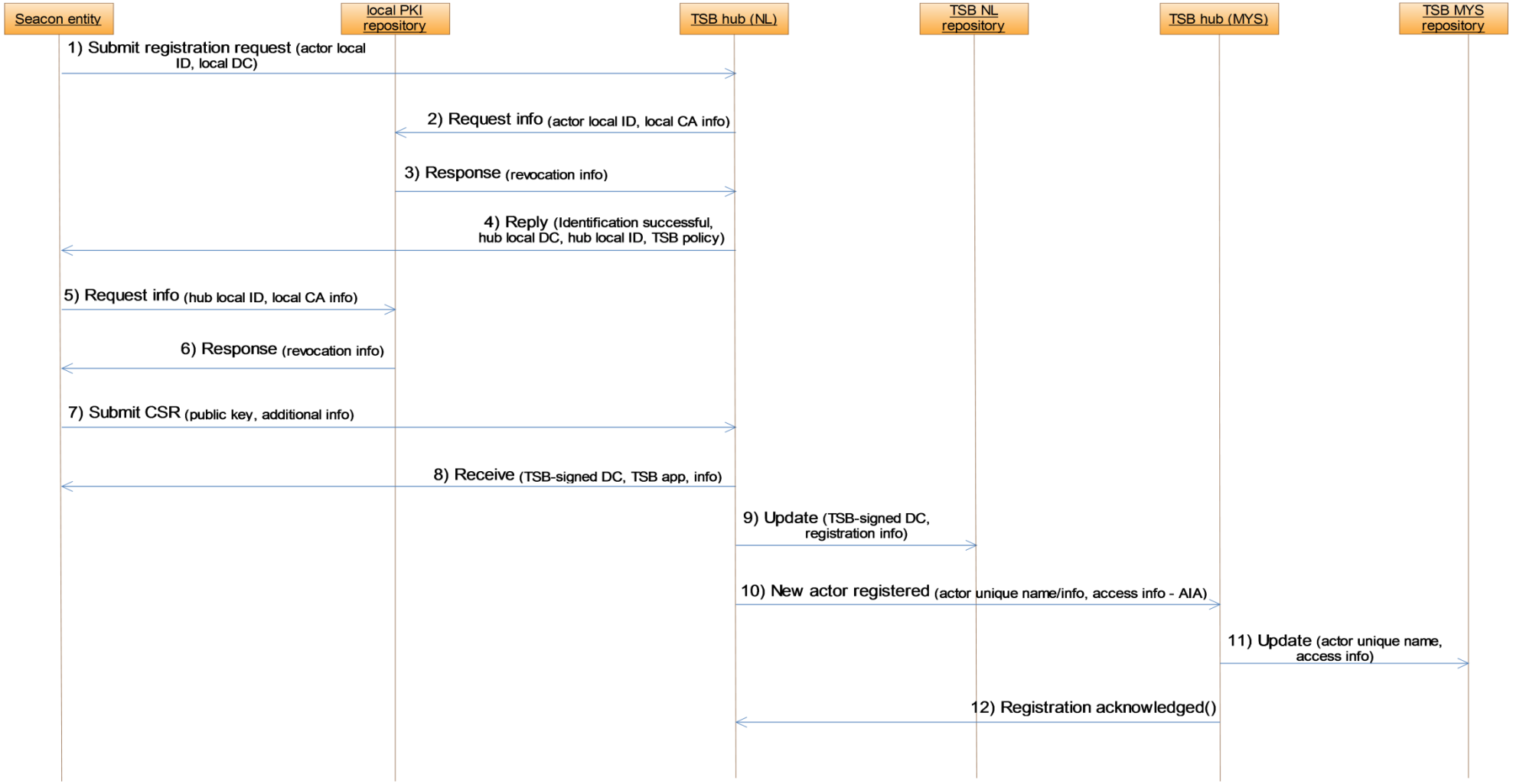

Figure 3.7: TSB initialization protocol

Before we describe this case of the initialization protocol with more details, we will first provide some general remarks. As discussed, it is important that the particular actor is a part of an existing local trust chain. Consequently, the TSB knows that the actor has already been successfully registered in a local trust domain (eg. a local PKI). Therefore, it is sufficient to successfully validate his credentials in order to guarantee that the perceived identity is true. In addition, important information about the actor is also contained within his local digital certificate and perhaps also through the local PKI repository. In this sense, the initialization process is significantly simplified and can be automated.

Protocol description

In order to register to the TSB, the Seacon entity must first provide all relevant information so that it can be identified by the corresponding TSB hub. In this aspect, the actor sends his registration request, along with his Digital Certificate signed by a local CA, his local identification number (if applicable) and additional information related to the actor, for instance the reasons for subscribing to the TSB services, or any particular capabilities he might possess. Upon reception, the TSB hub checks the validity of these credentials through the common TTP (in this case a local CA). By having access to the public key of the corresponding local CA via the local PKI repository, the TSB hub is able to verify the digital signature on the actors' certificates. It should be obvious that by gathering multiple certificates from local CAs, the necessary chain of trust is guaranteed, since the TSB is simultaneously registered in every domain and is therefore able to validate the certificates local actors have obtained by CAs in their respective domains, as described in section 3.2. In addition, the TSB can obtain additional information about the actors through the local repository. After the actor identification has been completed successfully, the TSB responds to the actor and sends its own credentials, so that the TSB's identity can be also validated. This is done in a similar manner. In addition, the actor also receives the TSB policy, which contains important information, for instance a list of acceptable algorithms for the creation of the key pairs. After the identity of the TSB hub has been established (steps 1-6 can be actually viewed as a simplified SSL handshake sequence, assuming that this process is done via the web), the Seacon entity generates the key pair(s) and submits a Certification Request (CSR) form, containing the generated public key to be certified, plus additional information (for instance capabilities or existing e-mail addresses and DNS spaces to be added at the "Subject Alternative Name" field of the certificate). Subsequently, the actor receives his certificate signed by the TSB and the local TSB hub updates the local TSB repository with the certificate containing the public key and additional information.

In order for the certificate to be accessible by partners in other regions, the local TSB hub also informs the other hubs (in the presented example this is limited to the Malaysian hub only, since our focus has been on two regions until now) about the newly registered actor and sends its unique name along with accessing information (a URI for instance, in the same way as it is stated in the AIA certificate extension). It should be noted that the certificate itself is stored only at the local TSB repository; nevertheless the necessary information in order for the certificate to be retrieved in the future is stored in all TSB repositories in case it needs to be accessed in the future. In this sense, each hub is responsible of maintaining/updating only the certificates of local actors, thus making certificate management much more efficient compared to a scenario where all certificates

are available in all TSB repositories, and less risky compared to a single / centrally managed repository (which would be a single point of attack and also raise manageability concerns).

3.4.2 Information exchange scenario

After the initialization process has occurred and assuming that each actor in the supply chain has been successfully registered to their local TSB hub, secure information exchange can take place. We will now present an example of such exchange of information, in the context described in chapter 2. As mentioned, information can be exchanged among partners both via e-mails and via web-based client server communication.

E-mail communication

We will now discuss how TSB-enabled functions can facilitate secure information exchange, for instance between Seacon and the Malaysian Freight Forwarder. We will assume that transmission is done via the SMTP in a MIME format (i.e. the SMTP/MIME standards are employed) in order to allow for the transfer of non-ASCII messages, such as programs or other types of documents, and that supporting applications are installed in both places (Tanenbaum & Wetherall, 2011). It consists of two main phases – encryption and decryption processes – and the TSB role is prominent for key/certificate retrieval purposes.

The first phase goes as follows:

- Seacon[1] creates a message, containing all necessary information, to be sent to the Freight Forwarder.
- Seacon produces a hash value of the message and signs it with his private key, thus creating a digital signature.
- For additional non-repudiation support, Seacon can request a time-stamp from the local TSB hub through the protocol described in Appendix A (not shown in figure 3.7).
- Seacon generates a symmetric key and uses it to encrypt the signed and time-stamped message.
- Seacon requests the FF's public key from the local TSB hub.
- The TSB-NL hub searched the local repository using the FF's unique ID. Since the FF is located in another region, the TSB-NL hub requests the certificate from the TSB-MYS hub. The TSB-NL hub is able to obtain the location of the FF's certificate as a result of the final steps of the initialization protocol.
- The Malaysian TSB hub retrieves the FF's certificate from its own repository and forwards it to the Dutch TSB hub.
- The Dutch TSB hub is validates the certificate (as all TSB hubs are cross-certified) and sends it to Seacon. (The hub also signs this certificate so that it can be subsequently validated by Seacon, which trusts the Dutch hub directly).
- Seacon sends the encrypted message, along with the encrypted symmetric key to the FF.

[1] By the notions "Seacon" or "FF" we refer to a specific entity (and the corresponding system) within these companies, for instance. a manager's terminal or a server.

The second phase goes as follows:

- The FF receives the encrypted message and symmetric key and uses his private key to decrypt the symmetric key.
- The FF uses the symmetric key to decrypt the message.
- The FF retrieves Seacon's public key / certificate in the same manner as Seacon retrieved the FF's DC previously (through the collaboration of both hubs). Since in essence the process is the same (the hub roles are reversed now), this is not described in details again.
- The FF generates a hash value of the message and uses Seacon's public key in order to compare the values, thus ensuring the message's authenticity and integrity.
- If applicable, the Time-Stamp applied by the TSB is also validated.

Figure 3.8 presented below, visually demonstrates this communication example. Another demonstration, which provides more details for the encryption / decryption processes, can be found in Appendix 3C.

Finally, since communication between Seacon and the FF is normally assumed to be done via the web, a web-based communication scenario can be also found in Appendix 3D.

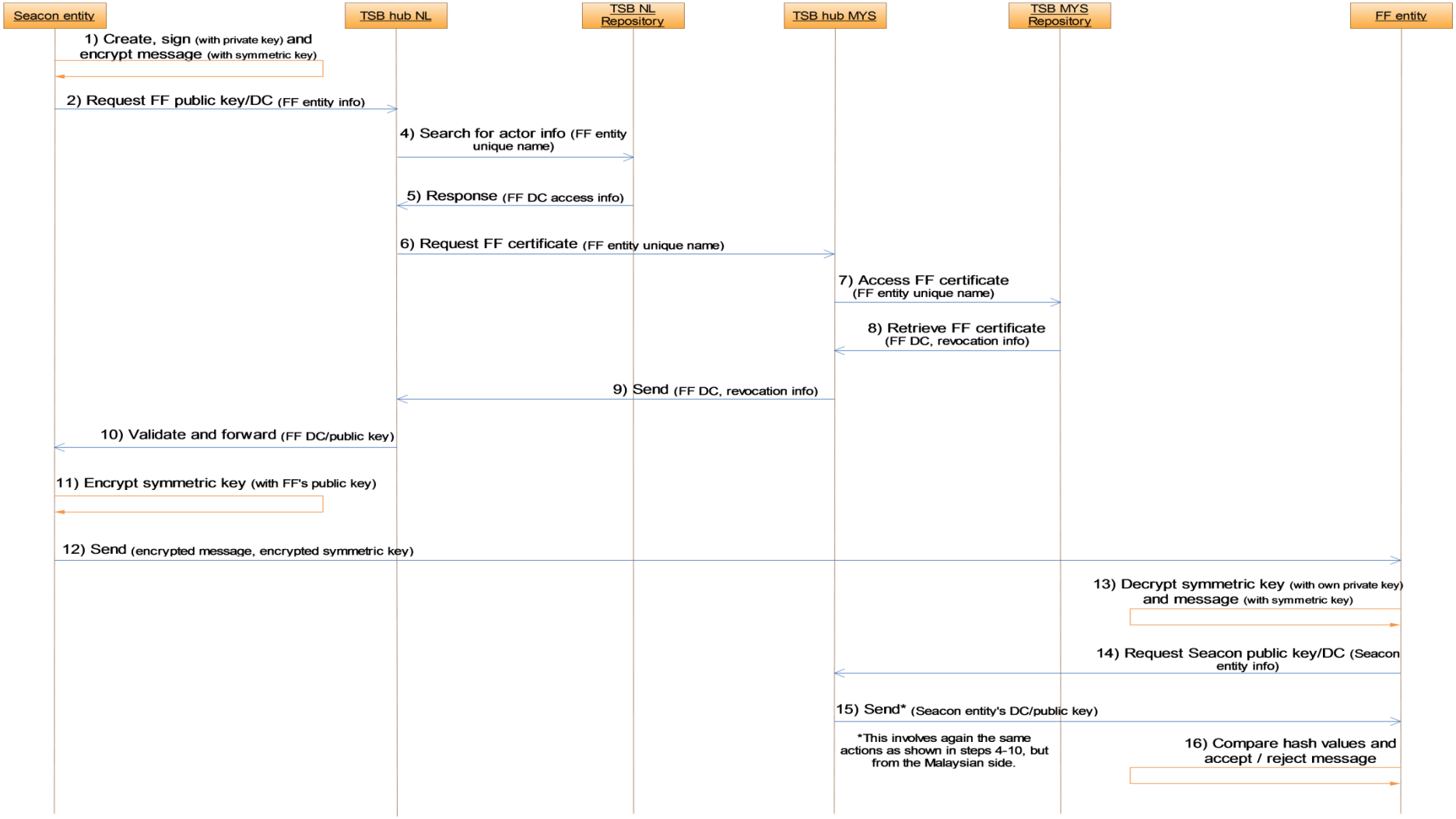

Figure 3.8: e-mail communication

3.5 Conclusion

In chapter 3 we began by further addressing the second sub-question, again with the main focus being on the functional/technical design requirements, which were elaborated and high level solutions for the establishment of a trusted global identity were provided. The solutions for meeting the functional requirements were analyzed in details throughout the rest of the chapter, by addressing the third sub-question, which regards the constituents of the TSB architecture.

The TSB was first examined from a broader perspective, by showing that it is in fact a distributed concept. We have argued that in order to provide a trusted identity to actors across different regions worldwide, the TSB is not a single organizational entity, but rather consists of "hubs" distributed throughout the globe. In this aspect, these hubs can be regarded as "trust anchors" in a given region and, in addition, they are interconnected through cross-certification means. Through this interrelation between hubs it is possible for the TSB to gain its power and authority globally.

We then examined the components of the TSB architecture in more details. On a high level the TSB architecture consists of physical/organizational entities, the TSB application, databases and digital components. In addition, we demonstrated how these components are utilized in order to meet the basic requirement for the provision of a trusted global ID. The first and most important step is the *initialization protocol,* which involves the secure identification of actors within the international supply chain, their registration and TSB certification. It was stated that it is essential for an actor to be part of an existing local trust chain (eg. a local PKI) in order to be successfully registered to the TSB. In addition, we have shown that the TSB "converts", in essence, the local certificates into a uniform TSB certificate and that the newly issued certificate is stored only at the local TSB repository, while all TSB repositories are updated with the necessary access information for future retrieval by actors in different regions. Finally, we have also presented a simple example of information exchange between actors located in different regions, showing explicitly how the two hubs mediate in the process. To sum up, the role of the TSB is most prominent both during the initialization process and during the actual exchange of information; however it is also important that each hub efficiently manages the certificates issued to actors within the same region, in a similar manner as CAs do.

CHAPTER 4: Risks and security controls

4.1 Establishing the risk assessment context

In the previous chapters we have described several issues concerning the information exchange between supply chain partners in a given scenario. We have also discussed how the TSB architecture can be an effective solution towards securing the exchange of information by providing trust. However, the TSB itself is not yet secure as a system. By having this in mind, we defined the requirement for internal TSB security in the previous chapters. In this chapter we will take a closer look at the potential risks associated with the operation of the TSB system and propose the necessary set of security controls that can minimize such risks and ensure that the TSB will function smoothly and efficiently.

Before we present our proposed risk assessment methodology, it is important to establish the context in which the assessment will take place. We have argued that the TSB's main purpose is to provide trust to supply chain partners. This is accomplished through various functions as described in chapter 3. First, the effective provision of trust heavily depends on the proper identification and TSB certification of actors, as described in the initialization protocol (fig. 3.7). In addition, actors rely on accessing the TSB databases (repositories) in order to communicate with their partners as described in the communication scenarios (eg. fig. 3.8). Moreover, the TSB hubs also perform functions independent of the actors (such as key and certificate management). Finally, the TSB hubs may also communicate and exchange information between each other (for instance managing directories and updating repositories with information related to actors subscribed in different regions), or for other organizational purposes. Figure 4.1, presented below, provides an overview of the information flow between the system elements for the aforementioned processes and serves to define the context of the risk assessment.

It should be made clear that figure 4.1 does not depict the information flow between Seacon and the FF; this was described in figure 2.5. Figure 4.1 rather describes the information flows related to the TSB processes which were summarized earlier and are essential within the TSB architecture. In addition, we must point out that the focus of our risk assessment will not expand on components external to the TSB architecture. For instance, figure 4.1 does not depict the information flow between the TSB hubs and the local CAs (or within the CA system), which is a part of the initialization protocol. The reason for this is that it is the responsibility of local CAs to establish a secure communication path with all relying entities (in this case both the TSB and the actors) and also guarantee the integrity and confidentiality of the certificates they issue. As a result, establishing the risks and security controls related to local CAs is out of our scope. In addition, dealing with the internal systems of the actors is also excluded from our analysis. Obviously, an actor sending incorrect information is something that cannot be managed by the TSB. In order to reduce such incidents, it is the actors' responsibility to take extra care of the information they intend to send. The data pipeline concept also helps towards this direction by reducing the amount of times data is exchanged. Sending incorrect information may result from different

things. It can be a result of employee carelessness, organizational system malfunctions and accidents (Smith, et al., 2007). In any of these cases it is the responsibility of the employees to ensure that the data to be sent is free of errors. Less frequently it can also be a result of principal-agent relationship between partners, meaning that the sender might deliberately chose to withhold or alter the information before it is send to his partner for personal gains. Finally, vulnerability in the system of one of the involved actors might be exploited by an external threat, thus resulting in unknowingly sending incorrect information. In such cases, it is the responsibility of the organizations and their own security systems that sensitive information is not tampered with.

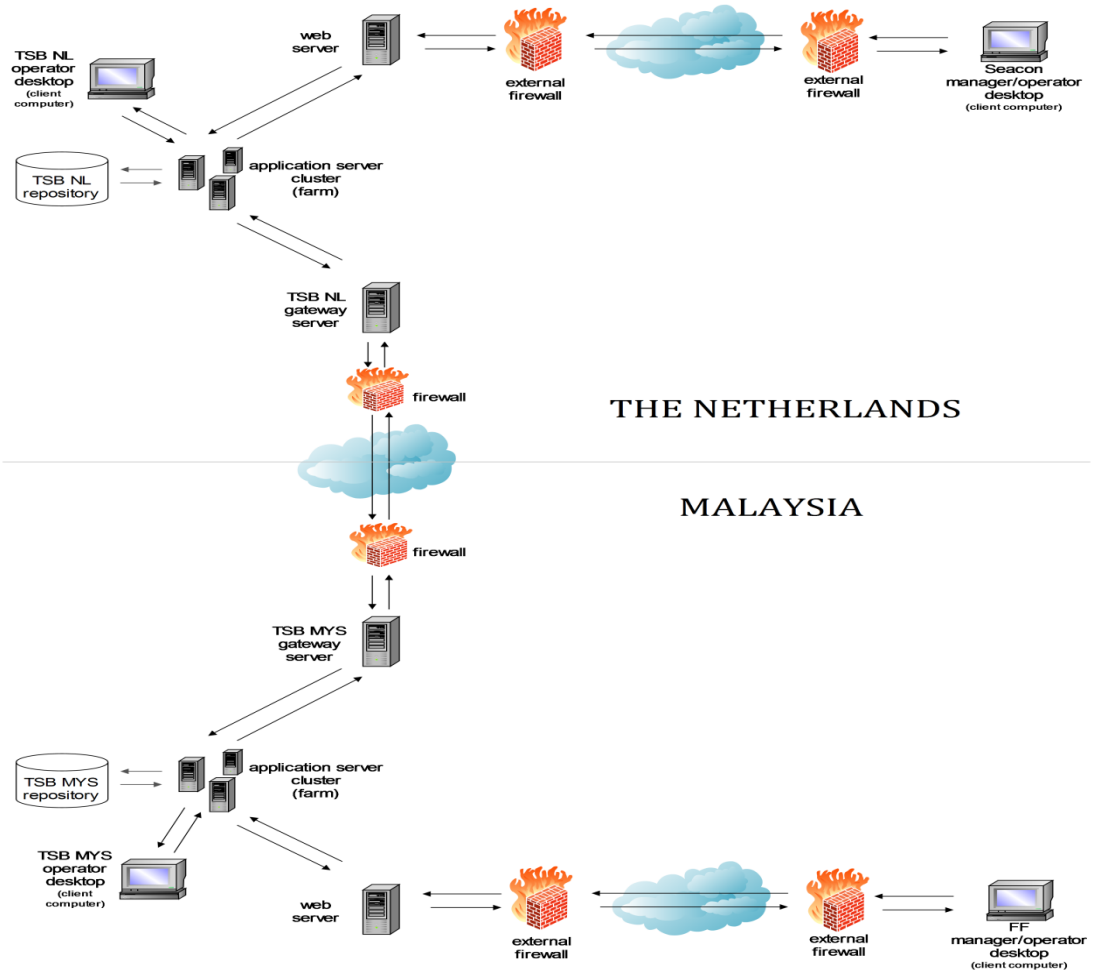

Figure 4.1 Information flows related to TSB processes

To sum up, the scope of our analysis will be to identify the risks associated with the TSB system, as well as with hub-to-hub and hub-to-entity communication (incoming communication), and determining the proper security controls that need to be in place in order to minimize the business impacts. Only then will it be possible for the TSB architecture to ensure that communication between the supply chain actors is done efficiently and securely.

Finally, we should also make clear that we are considering a risk assessment within an organization/system (the TSB) that does is not yet established. This has two major implications. The first is that there are various assumptions that need to be made with regard to the TSB-hub (fictitious) organization. Figure 4.1 summarizes these assumptions, in terms of the TSB infrastructure (eg. number and type of servers etc.). In addition, we must also make some assumptions regarding the "current" security controls within the TSB system, based on common security practices in similar types of established organizations. The second implication regards potential differences between different TSB hubs. As it is demonstrated in Figure 4.1, we assume that there are no differences across TSB hubs in terms of both their infrastructure and their business processes. This is an important implication, since a risk assessment within one TSB hub is sufficient and can be generalized for all other hubs. In reality, there might be some differences between hubs, for instance due to varying regulations and technology levels across different countries; nevertheless, all TSB hubs perform the same operations and can essentially be considered as one.

4.2 Risk assessment

4.2.1 High level methodology description

For the purposes of this thesis, we will carry out a risk assessment process, based on Microsoft's Security Risk Management Guide. It provides a proactive approach that can assist organizations with their response to all kinds of information security challenges. The high level procedure goes as follows (Microsoft, 2006):

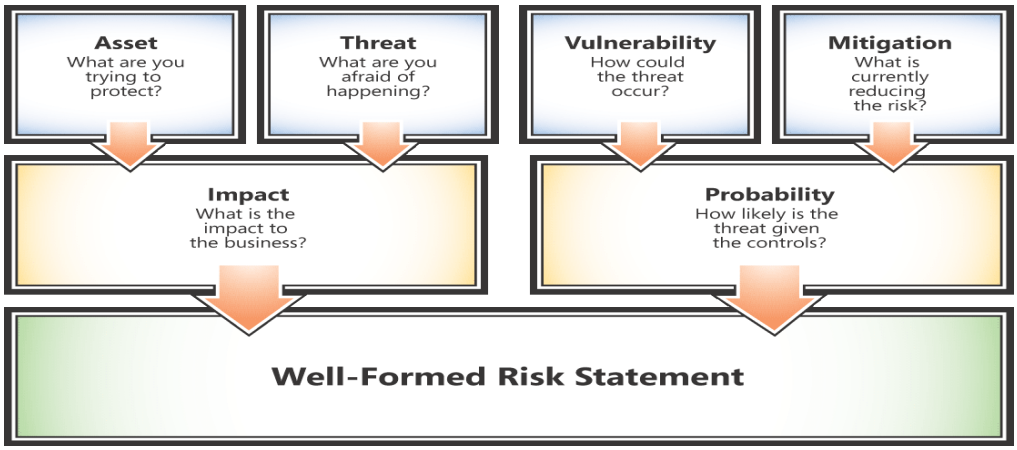

Figure 4.2: Risk assessment phase. Source: (Microsoft, 2006)

Since the TSB hubs are not established as organizational entities yet and, as a result, quantifying probabilities and monetizing business impacts will involve making many unnecessary assumptions, we will focus on the qualitative approach. The basic process for qualitative assessments is very similar to what happens in the quantitative approach. The difference is that comparisons between the value of one asset and another are relative, and participants do not invest a lot of time trying to calculate precise financial numbers for asset valuation. The same is true for calculating the possible impact from a risk being realized and the cost of implementing controls. In our effort to arrive in a well-formed risk statement, we will utilize the corresponding SRMG tools.

The next phases of Microsoft's SRMG involve several organizational processes and discussions among stakeholders to establish the proper security controls. Since this is quite a complicated approach, particularly considering the fact that we are dealing with an organization that does not yet exist, we will utilize the new Microsoft Security Assessment Tool, an automated tool that can facilitate the control selection phase. This phase will therefore combine the output of this tool (which is based on best practices across organizations similar to the TSB) with the risk statement findings. A more thorough description of the risk assessment and control selection phases is presented in Appendix 4A.

4.2.2 Detailed risk assessment and proposed controls

We will first provide some more information regarding the asset selection and classification. Starting with HBI assets, the first asset under consideration will be the TSB hub private key. Apparently, as it is also the case with all CAs, a potential compromise in the private key of the TSB hub will have catastrophic consequences both in direct financial losses and in terms of the TSB reputation and trustworthiness. As a result, any loss of integrity, availability, confidentiality, authentication and access control related to this asset can be devastating for the TSB operations and of course for the relying supply chain partners. This asset is an example of intranet data. The same considerations also apply to the supply chain actors' public keys, certificates and personal information (extranet data) and also critical infrastructure, such as data centers. Examples of MBI assets include TSB public key (extranet data), operational TSB data (intranet data) and the TSB application (infrastructure). Finally, examples of LBI assets are desktops and cell phones (infrastructure). Table 4.1 gives a detailed description of the asset classification based on the criticality of a certain security aspect being compromised.

ASSET	CATEGORY	IMPACT IN CASE OF LOSS OF:						BUSINESS IMPACT
		Integrity	Confidentiality	Availability	Authentication	Access control	Non-repudiation	
TSB private key	Intranet data	High	High	High	High	High	High	**HIGH**
Actor keys, DCs and personal info	Extranet / Internet data	High	Medium	High	High	High	High	**HIGH**
Data centers / servers	Hardware	High	-	High	High	High	-	**HIGH**
TSB application	Software	High	Low	High	High	High	Medium	**HIGH**
Operational TSB data	Intranet data	Medium	Medium	Medium	Medium	High	Medium	**MEDIUM**
TSB public key	Extranet / Internet data	High	Low	High	Low	Low	Medium	**MEDIUM**
Desktops	Hardware	Low	-	Low	Medium	Low	-	**LOW**

Table 4.1: Asset classification

The aforementioned assets are the ones being directly assessed. *At this point, we should make clear that there are several more organizational assets which should be part of a detailed risk assessment. Nevertheless, by classifying the assets both in terms of type (intranet data, extranet/internet data and infrastructure) and criticality, we can argue that assets that fall under the same category in both type and criticality can be considered to be exposed to similar types of risks.* For instance, apart from the TSB private key, highly critical intranet data such as passwords or financial information have similar properties and are more or less subject to similar threats and vulnerabilities. In this sense, when we assess the risks for each of the proposed assets, it is implied that similar results also apply for equally critical assets in the same category. We should also note that by "intranet data" we refer to data that are only accessible locally, while "extranet/internet" data are also accessible remotely, for instance by the supply chain actors which are subscribed to the TSB. Table 4B.1, in Appendix B, gives a detailed overview of the asset clustering based on these two properties.

Following the asset classification with regard to business impact, the most prominent sets of threats and vulnerabilities (for each applicable defense-in-depth layer of every aspect) are determined. Common threats and vulnerabilities are available in various external sources. Although it is out of our scope to provide extensive references on this issue, lists of common threats and vulnerabilities as described within Microsoft's security risk management guide are presented in Appendices 4C and 4D respectively. A much more comprehensive vulnerability list, containing more than 50.000 identified and up-to-date vulnerabilities can be also found through the NIST National Vulnerability Database v2.2 (NIST, 2013). For the selection of threats and vulnerabilities to consider in the assessment, we will rely both on our own judgment for relating these lists to the TSB context and also on the output of the automated MSAT tool. The basic inputs for the MSAT tool (in order to reflect to an organization similar to the TSB) can be found in Appendix 4E.

Finally, regarding the selection of current controls, in order to assign a final probability to the impacts occurring, we will first consider some important things discussed in the previous chapter. For instance, when considering the risks associated with the keys of supply chain actors, it is important to have in mind that, by definition, the actors' *private* keys are stored within their own systems and, as such, they are not a concern. Nevertheless, in addition to these considerations, we are also going to assume that certain (basic) security controls are in place within the TSB-hub system, for instance anti-viruses, firewalls and certain internal-authentication mechanisms.

Table 4.2 provides an overview of the risk assessment for the identified assets, taking into account all the issues and assumptions that have been discussed so far in this chapter. Obviously, the list of all combinations of threats and vulnerabilities for a given asset / DID layer could be endless. We have therefore selected to include some of the most representative risks that a TSB hub could face. In addition, we propose additional controls (mainly based on the MSAT tool results) in order to further mitigate the risks and fully address the security requirements for each asset as a whole (as described in table 4.1). A more detailed table (but still limited to the most prominent/representative risks) is given in Appendix 4F.

Asset					Exposure							
Risk ID	**Asset Name**	**Asset category**	**Asset Class**	**Applicable Defense-in-Depth Layer(s)**	**Threat Description**	**Vulnerability Description**	**Exposure Rating (H,M,L)**	**Impact Rating (H,M,L)**	**Current Controls Description**	**Probability (H,M,L)**	**Summary Risk Level (H,M,L)**	**Proposed controls**
1.2.1	TSB private key	Intranet data	HBI	Network	Unauthorized access to the hub's intranet	Connection of unauthorized local client to hub's intranet due to outdated configuration of perimeter defense mechanisms	L	**M**	1. Separation of critical internal hub resources from resources accessible to end entities. 2. No remote accessing of critical internal hub resources. 3. Intranet firewalls and intrusion detection systems in place. 4. No wireless connectivity to hub's intranet.	**M**	**M**	1. Deploy firewalls and other network-level access controls at each location and frequently test and verify that they are working properly. 2. Ensure that network-based intrusion detection systems' signatures are kept up-to-date.
1.3.1	TSB private key	Intranet data	HBI	Host	Unauthorized access to critical intranet data such as the TSB's private key through theft of credentials	Theft of credentials off managed LAN client via outdated configuration of antivirus signatures, host configuration, or outdated security patches	M	**H**	1. Restrict access to this data only to the TSB-hub senior managers. 2. Antivirus update and patches enforced on LAN every few hours - narrowing compromise of host during time window of exploit vs. patch. 3. E-mail notices to patch/update.	**H**	**H**	1. Multi-factor authentication mechanisms for highly-authorized individual's accounts. 2. Adding anti-virus client in the default workstation build environment. 3. Keep different types of data in separate places depending on their criticality.
1.4.1	TSB private key	Intranet data	HBI	Application	Unauthorized access to critical intranet data such as the TSB's private key by employees through improper exploitation of the TSB hub application (which accesses the TSB private key for the process of actor certification)	Exploitation due to code weakness	M	**H**	1. TSB application developed in-house. 2. Regular provision of patches and updates. 3. Authorization mechanisms that provide access to sensitive data and functionality only to suitably permitted application users.	**M**	**H**	1. Regular auditing of application configuration. 2. Quick response to identification of critical code weaknesses. 3. When a patch is made available, testing in lab-conditions is essential. 4. Collaboration with experienced third-party application developers to review the application. 5. Encrypt all sensitive data prior to transmission to other components.

1.5.1	TSB private key	Intranet data	HBI	Data	Unauthorized access to critical intranet data such as the TSB's private key through theft of credentials	Theft of credentials **via** non-technical means (eg. eavesdropping) by trusted employees.	H	**H**	1. Restrict access to this data only to the TSB-hub senior managers. 2. Background checks on employees	**L**	**M**	1. Multi-factor authentication mechanisms for highly-authorized individual's accounts. 2. Encrypt all sensitive data stored, through the strongest encryption algorithms, such as 3DES or AES. Use a key length of 128 bits at minimum (1024 bits for AES).
2.2.2	Actor keys, DCs and info	Extranet / Interent data	HBI	Network	Disclosure of actor information through unauthorized connection to the hub's network	Unauthorized connection of **remote** client to hub's network due to outdated configuration of internal perimeter defense mechanisms and absence of segment filtering.	M	**H**	1. Internal firewalls and intrusion detection systems in place. 2. VPN for remote-user-access connectivity based on Secure Sockets Layer (SSL) is currently being used to secure access. 3. Network controls are in place to restrict access to only what is required for each third-party connection.	**H**	**H**	1. Deploy site-to-site connectivity based on IPsec technology. Configure network access lists and user access lists for restricting access to necessary corporate resources. 2. Use segmentation to separate specific extranets from different user access and restrict access between network segments. 3. Deploy one or more DMZs (demilitarized zones) as part of a systematic and formal firewall development. 4. Place all Internet accessible servers there. Restrict connectivity to and from the DMZs.
2.4.1	Actor keys, DCs and info	Extranet / Interent data	HBI	Application	Access to customer data by a party outside the TSB community via unauthorized use of the TSB end-entity application	Unauthorized use of the TSB application via poor authentication mechanisms.	H	**H**	1. TSB application is given to actors after they successfully complete the initialization protocol. Passwords are selected by actors.	**M**	**H**	1. Implement an authentication mechanism whose strength is commensurate with data criticality. Strong passwords should be 8 to 14 characters in length, with alphanumeric and special characters. 2. Minimum length, history maintenance, lifetime, and pre-expiration of passwords should all be set to provide additional defenses to password strength. 3. Account lockout, after 10 failed login attempts, should be enabled. 4. Role-based access controls should be enforced at the application interface. 5. All attempts to obtain access without proper authorization should be logged.

3.1.2	Data centers / servers	Physical Infrastructure	HBI	Physical	Damage or theft of the equipment by unauthorized access of third parties.	Unauthorized access to critical infrastructure equipment due to poor physical security procedures	H	**H**	1. Alarm systems installed in equipment rooms to detect break-ins 2. Data centers are in a locked room with restricted access.	**L**	**M**	1. Institute physical access controls against unauthorized personnel, such as employee and visitor badges. 2. Increase staff awareness of the personnel access control policy and encourage the challenging of unrecognized individuals.
3.3.2	Data centers / servers	Physical Infrastructure	HBI	Host	Setback of operations due to database/server being unavailable	Denial of service due to poorly defined procedures in case of high load or DDOS attacks.	H	**H**	1. Recovery and backup mechanisms	**H**	**H**	1. A more proactive approach is required. To ensure high availability for critical databases and servers, clustering mechanisms can be deployed. 2. Hardware load balancers can be deployed in front of web servers to achieve higher availability.
4.4.1	TSB application (as an asset itself)	Infrastructure	HBI	Application	Disruption of operations due to application malfunctions.	Malfunctions and glitches due to poor application development practices.	H	**H**	1. TSB application developed in-house. 2. Application development fully documented	**H**	**H**	1. Regular back-up of applications and maintenance of in-place contingencies 2. Regular provision of patches and updates
5.4.1	TSB operational data	Intranet data	MBI	Application	Disclosure or manipulation of operational data via the TSB-hub application.	Manipulation or loss of data due to missing patches	M	**M**	1. The development team identifies critical patches and applies them as soon as possible.	**M**	**M**	1. All applications should be periodically evaluated for security, backed up regularly, fully documented, and have contingencies in place in case they fail. 2. If there are any known application vulnerabilities that do not have available patches, determine when a patch will be available and develop an interim mitigation plan to address that vulnerability.
6.5.1	TSB public key	Extranet / Interent data	MBI	Data	Disruption of actor-to-actor communication due to manipulation (or inability to retrieve) the TSB public key	TSB public key incorrect or lost due to mistakes and poorly defined procedures	H	**H**	1. Regular data back-up.	**M**	**H**	1. Define roles and responsibilities among employees and promote security awareness in order to avoid costly mistakes. 2. Immediate update of the database if a compromise of the TSB public key is suggested by the actors.
7.3.1	Workstations	Physical Infrastructure	LBI	Host	Unauthorized access to personal employee workstations and data	Workstations can be left unattended by careless employees	L	**L**	No controls	**M**	**L**	1. All users should have a password-protected screen saver with a short time-out period.

Table 4.2: Detailed risk assessment and controls

4.2.3 Deployment of (technical) security controls

The deployment of the technical internal security controls for the TSB hubs aims to protect the assets under consideration and is based on the results of our risk assessment, while also complying with the (NIST, 2009) security controls guidelines. Hence, each security control is appropriately deployed in order to minimize the identified risks.

With regard to the incoming traffic from remote entities (eg. other hubs or supply chain actors) via the TSB application, a VPN tunnel should be established, as it supports data-in-transit encryption protocols, such as the SSL protocol (Tanenbaum & Wetherall, 2011). The TSB-issued certificates can be thus used for the purposes of an SSL handshake. The main reason that necessitates this approach is that there is highly sensitive information being exchanged (such as keys and actor certificates), which should be encrypted at all times. The TSB gateway server serves as the endpoint of the VPN tunnel, where the authentication of remote entities takes place.

Based on the proposed controls by the MSAT tool, and also in line with the NIST guidelines, network segmentation must also take place, in order to separate critical resources and hosts from the non-critical ones. In this aspect, a DMZ is established by installing both an external and internal firewall, thus separating this zone from the hub's intranet. By defining highly restrictive rules for the firewalls, both the DMZ and the hub's intranet vulnerabilities to unauthorized entry are reduced (at the Network DID layer). In addition, according to (NIST, 2009), Network-based Intrusion Detection Systems should be in place next to the external and internal firewalls, in order to detect attempts for unauthorized access to both the DMZ and the hub's intranet in a timely manner.

With regard to the deployment of hosts, it is recommended that the hub's web servers should be placed within the DMZ, in order to protect the application servers and critical databases, in the event of a successful intrusion (NIST, 2009). The latter are placed within the hub's intranet. To prevent unauthorized access to these hosts, both anti-virus and host-based intrusion detection systems should be installed and periodically updated within the host environment. Due to the fact that viruses and worms affect the application layer of computer systems, anti-virus solutions must be also properly installed on workstations as well, according to the SI-3 section (NIST, 2009). Also, in cases of high demand, the use of hardware load balancers or traffic managers serves to increase the availability of hosts, by efficiently distributing the workload among them.

Finally, due to the sensitivity of the data stored within the TSB databases, all data should be encrypted with a strong algorithm, such as 3-DES or AES, according to both the NIST guidelines and the MSAT recommendations. In addition, data-in-transit within the TSB network should also be encrypted with one of the aforementioned algorithms.

Based on these recommendations, figure 4.3 shows the TSB system network with the proposed (technical) controls in place. Apparently, there have been additional controls proposed during the risk assessment (eg. physical or organizational), but these cannot be depicted.

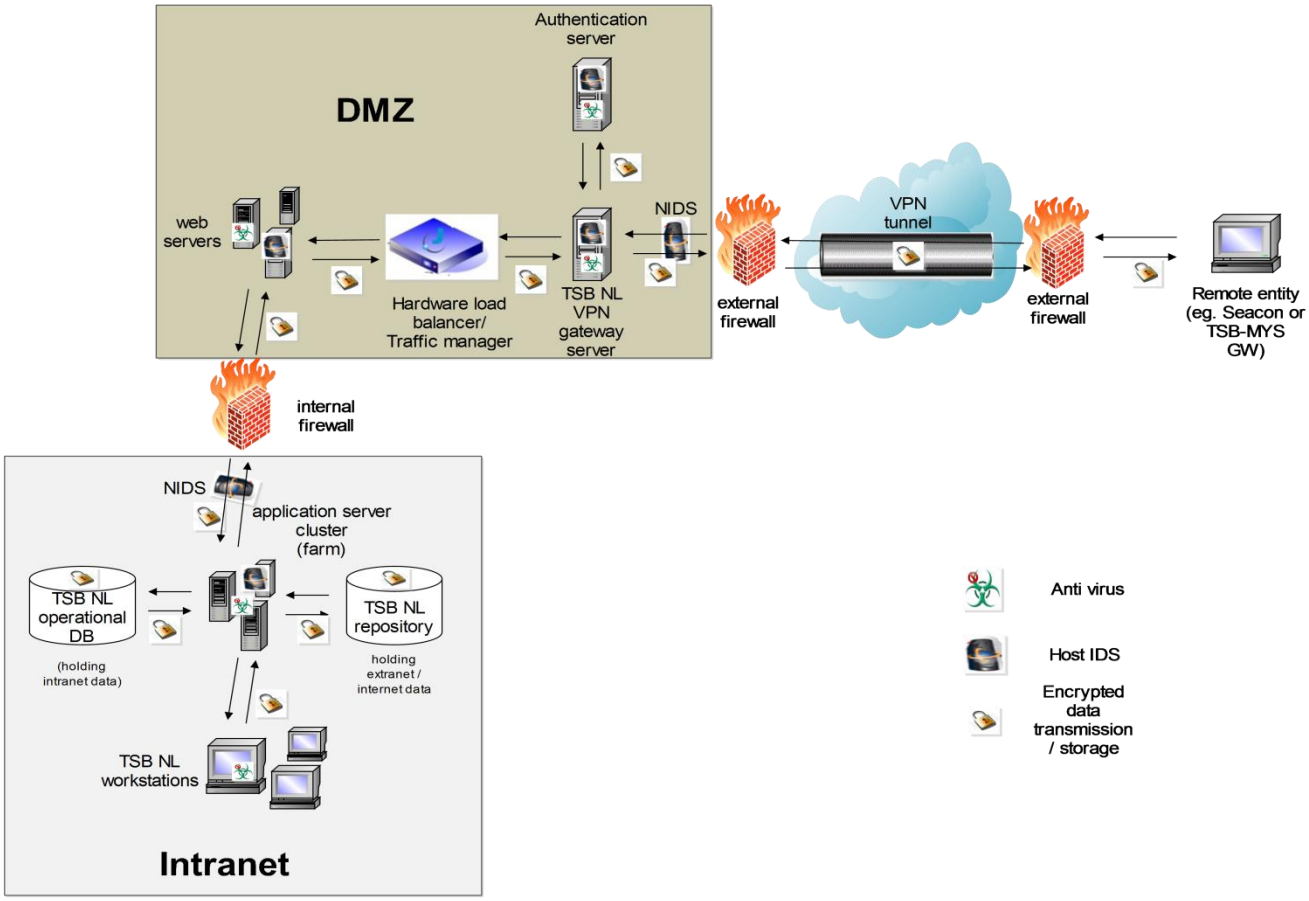

Figure 4.3: TSB system with (technical) security controls

4.3 Conclusion

In this chapter we have dealt with the TSB internal security concerns, thereby addressing the fourth sub-question. We first established the context of the security risk assessment that was performed, which did not include the assessment of systems external to the TSB system. In this sense, we have argued that local CAs, as well as the international supply chain actors, should be responsible for securing their corporate networks. In addition, since we have argued that TSB hubs are essentially the same, we focused the risk assessment process on one hub, as similar considerations eventually apply to all of them.

The risk assessment process was made through a qualitative approach, since the TSB hubs are not established as organizational entities yet. Our main focus was to identify the risks related to the loss of the availability, integrity and confidentiality (primarily) and also authentication/authorization and access control of critical TSB assets. Finally, based on the recommendations in (NIST, 2009) and the output of the MSA Tool for the identified risks, we proposed a set of security controls for securing the TSB hub systems.

CHAPTER 5: Validation and generalization

In this final chapter, we begin by validating the proposed TSB solution, particularly considering to what extent our design requirements have been met. In addition, we present our views for a generalized TSB solution in a global scale.

5.1 Validation

Before we describe the validation process of the TSB solution with regard to the design requirements, we need to clarify two things. First, it should be evident by now that the main focus of this Thesis was to present how the TSB is able to provide a trusted global identity, particularly considering the international supply chain environment. In this sense, the main focus in this section will also be in validating the functional/technical requirements. Second, to avoid any misinterpretations we must also make clear that the TSB security requirements reflect on the security of the TSB as a system itself. To be more specific, the (functional) requirement for ID verification (in other words facilitating authentication between supply chain actors) should not be confused with the (security) requirement for authentication, which is related to the internal TSB system (eg. authentication for using the TSB application, or for accessing internal resources by TSB employees).

5.1.1 Preparations

In this section we describe the preparation process that preceded the validation of the TSB solution. The validation was done from a theoretical perspective through expert opinions, as testing the TSB solution in a real environment required resources and time that were not within our reach. In order to refine the validation process and target specific points of interest, it was essential that a set of validation points/criteria should be defined in advance, prior to contacting the experts. These criteria were selected to reflect the overall design of the TSB architecture, as well as its significance and relevance to the research problem and the international supply chain case under consideration. A more comprehensive description of the validation criteria is provided in the next section.

Regarding the selection process of the experts that participated in the validation process, these included people both within the industry and the Academia, including researchers within Delft University of Technology. Apart from the people who were involved in this project from the beginning (Semir Daskapan – TU Delft TBM faculty, Jan van den Berg – TU Delft TBM faculty, Christian Doerr – TU Delft EWI faculty) and have provided invaluable feedback throughout the whole process, experts with no direct involvement in the creation of the TSB architecture were also contacted in order to reduce bias. More specifically, we were able to contact industry experts Wout Hofman (TNO senior innovator) and Tony Bos (CYBBOS founder and CEO), as well as academic experts (from the TU Delft TBM faculty) Potchara Pruksasri and Wolter Pieters. During our initial contact with each expert, a short presentation of our work, followed by a list of questions and points of interest related to our set of validation criteria were provided to them. Mostly depending on their availability, the experts were reached either in person, thus conducting a face-to-face interview, or via e-mail communication. Regardless of the approach, all experts had related academic

knowledge or experience and, as a result, they were able to provide valuable comments on our work. Finally, during the interviews particular emphasis was placed in certain criteria, depending on the specific field of expertise and personal interests of each expert. Nevertheless, and looking at the totality of interviews, all validation points were addressed.

5.1.2 Description of the validation criteria

The validation criteria were defined prior to contacting the experts and were selected in a way to reflect all the design aspects of the TSB, as well as to determine the significance of the overall TSB architecture.

Looking at the TSB solution as a whole, our first criterion regards its **significance** and contribution to the research problem as defined in chapter 1 and also its **relevance** to the international supply chain case as described in chapter 2. Regarding the latter, determining the correctness of the described case was also of interest.

Since the functional/technical design of the TSB was the primary focus of this Thesis, the second validation criterion is also the most prominent one. It regards the **technical feasibility** of the TSB, which essentially comes down to meeting the functional/technical design requirements.

In addition to the technical feasibility, we were also interested in determining the **flexibility** of the TSB solution in supporting information exchange within a more complex environment than the example provided in section 3.4.2. This was the third validation criterion.

Regarding the security design, the **correctness** of our solution to meeting the internal security requirements was the fourth validation criterion. Despite the fact that a TSB hub organization does not exist, and as a consequence we are dealing with a fictitious network, the experts were still asked to comment on it and also give their insights on other security related concerns.

Finally, and although this was not initially planned as it was out of our scope, all experts were also keen on commenting on the **usability** of the TSB, particularly regarding a global TSB implementation and specifically focusing on potential legal and organizational implications. As a result, this was added as final validation criterion.

5.1.3 Validation results

5.1.3.1 Significance and relevance

To begin with, the significance of the TSB solution is evident, both taking into account the implications of the trust domains problem on organizations and also the inefficiency of current trust models to deal with it. A particular remark that was made during the validation process regarded the comparison of the TSB with modern interoperability solutions that are currently implemented to deal with the problem (most prominently the solution of root CA certificates being embedded into popular web browsers). Based on this remark, the problems with this approach were made more explicit in chapter 1. Regarding the international supply chain case, it was pointed out that a successful implementation of a

TSB solution could indeed solve many issues regarding the information exchange between organizations in different countries. In addition, the description of the case scenario and the related business processes and information flows was found to be quite detailed and in line with reality.

5.1.3.2 Technical feasibility

Overall, the functional/technical design of the TSB architecture as described in chapter 3 was positively received and the TSB solution with regard to the establishment of a trusted global Identity for the international supply chain actors was found technically feasible. We will now provide more details on how the functional design requirements have been met, along with relevant comments by the experts.

ID verification

The provision of a trusted ID has two facets. First, the TSB should be able to securely identify supply chain actors. In order to do so, we have argued that actors, as well as the local TSB hub, should already be a part of an existing local trust chain (for instance a local PKI), so that the TSB can verify their identity (and vice versa) by the means described in the initialization protocol. Second, actors should be able to securely identify each other when they wish to share information, so that the messages' authenticity and integrity can be guaranteed. The first step to achieve this is through the issuance of the TSB certificates, again within the initialization protocol. The second step regards the search and retrieval of these certificates, which is described in details in the e-mail communication example. In order to facilitate the process of retrieval, every hub's repository is updated with access information regarding issued TSB certificates by other hubs upon registration. Finally, in addition to the issuance of the certificates, the TSB is also responsible for providing key and certificate life-cycle management functions in order to guarantee that trusted IDs are not compromised in the future, as described in appendix 3A.

In addition, although the requirement for capability verification has not been addressed in details, actors can declare any capabilities they possess by submitting the necessary information upon their initial TSB certification. By this, the TSB hub can make use of a certificate extension in order to vouch for these capabilities. Again, this is also possible through the initialization process.

Unique naming

With regard to the requirement for a unique global name, all necessary information is provided by the actors (including actor details and additional information to be used in the "SubjectAlternativeName" extension, if applicable) by submitting the CSR form as described in the initialization protocol. The local TSB hub is responsible for keeping all the necessary information in order to create a globally unique ID, in accordance to our proposition in section 3.1. The proposed convention ensures the uniqueness of identity (as it is based on the uniqueness of the public key and it is particularly essential for the efficient retrieval of actor certificates, as shown in the e-mail communication example), while also retaining a degree of local meaningfulness.

During the validation process, it was pointed out that a validity period should be also established for each name. This is important both when considering the dynamic

environment surrounding the TSB, but most importantly because the validity of the identity depends on the validity of the certificate (as the name contains the hash function of the public key). Since each certificate is issued and considered valid for a certain period, the same should apply for the name of the certificate holder.

Dealing with different trust foundations

The ability of the TSB to deal with different types of local trust and, consequently, to recognize different types of local certificates is directly related to the distributed TSB concept, as described in section 3.2. In this sense, these issues are addressed directly upon anchoring the TSB hubs in local territories, thus becoming a part of the local chain of trust. Subsequently, the TSB hubs are able to validate the actors' local DCs (and vice versa) through the initialization protocol.

In addition, the experts argued that the **compatibility** of the certificates issued to actors in different regions by the TSB is of crucial importance. This requirement is also met, since all TSB certificates are based on the X.509 v3 format. Although the specific format of the issued certificates is a less important consideration (as long it remains the same for all regions), we still consider the X.509 v3 as the most viable choice, as apart from reliability, they offer the possibility of utilizing extensions for various purposes (for instance if an actor possesses a particular capability, or has additional naming preferences).

5.1.3.3 Flexibility

Although our proposed protocols were positively received and offer a quite dynamic solution for the provision of a global trusted ID, we have only examined the process of information exchange between two actors in isolation of their environment. Although this was done on purpose, since our main goal was to illustrate how the TSB is involved in the information exchange process between two actors, experts commented that the proposed solution is also very flexible.

To elaborate more on that, and in relation to the CASSANDRA project, it can be very often the case that one entity (employee) may act on behalf of its organization, or one organization can be authorized by another to retrieve information on their behalf. As an example, the Dutch customs (or the consignee) may request product or shipment information from the export side, which is held at the FF's database, and this information will be eventually available through Seacon's import-side dashboard. So in essence, Seacon is authorized by the Dutch customs to retrieve information on their behalf. This can be addressed through the use of "**Authorization Tokens**", as described in (Hofman & Bruijning, 2008). In short, this token is created to guarantee that Seacon is officially authorized by the Dutch customs (for a defined "validity period") to retrieve the information on their behalf and is digitally signed by both the customs and the local TSB hub. Subsequently, when Seacon requests this information from the FF, the Authorization Token needs to also be sent and validated (via the Malaysian TSB hub, in the same manner as with a TSB certificate) in addition to Seacon's own certificate. It is evident, therefore, that the TSB architecture can also support additional cases of information exchange within a more complex environment.

5.1.3.4 Correctness of the internal security design

As a general remark it can be noted that although a detailed risk assessment was performed in chapter 4 in order to derive the corresponding security controls for the internal TSB system, the validity and reliability of these results is inherently limited, since we are considering an organization that is not yet established. In this sense, the experts' contribution on the correctness of the solution was also limited. Before we present some of the most important expert comments, table 5.1 will serve to show how the internal security requirements for the TSB system as a whole have been met through the implementation of technical controls as shown in figure 4.3. We focus on both infrastructure and communication nodes, while examining them according to their network location, in order to avoid potential overlaps.

FOCUS	NETWORK LOCATION	Addressed Security requirements	Proposed security controls
Communications	Internet (external entity to DMZ)	Data integrity	VPN tunnel with data encryption
		Data confidentiality	
		Remote entity access control	
Communications	TSB network (within DMZ and intranet, and also between them)	Data integrity	Data-in-transit encryption
		Data confidentiality	
Infrastructure	DMZ	Access control	Incoming internet traffic routed via the external firewall
Infrastructure	DMZ	Access control	Deployment of Network-based IDS at the DMZ entry point
Infrastructure	DMZ	Data integrity	Placing TSB web servers within the DMZ
		Data confidentiality	
		Access control	
Infrastructure	DMZ	Host availability	Placing hardware load balancers to facilitate web-server availability
Infrastructure	DMZ	Remote entity authentication	Dedicated remote authentication server
Infrastructure	DMZ	Data integrity	Installing anti-virus software and host-based IDS in all hosts
		Data confidentiality	
		Host availability	
Infrastructure	TSB intranet	Access control	Incoming DMZ traffic routed via the internal firewall
Infrastructure	TSB intranet	Access control	Deployment of Network-based IDS at the intranet entry point
Infrastructure	TSB intranet	Local entity authentication	Multi-factor authentication
Infrastructure	TSB intranet	Data integrity	Keeping critical intranet data in a separate database
		Data confidentiality	
Infrastructure	TSB intranet	Data integrity	Stored data encryption
		Data confidentiality	
Infrastructure	TSB intranet	Host availability	Application server clustering

Infrastructure	TSB intranet	Data integrity Data confidentiality Host availability	Installing anti-virus software and host-based IDS in all hosts
Infrastructure	TSB intranet	Non-repudiation	Keeping logs of user access and data processing on the application and database levels

Table 5.1 Self-validation of internal TSB security design requirements

With regard to table 5.1, it must be noted that it only includes the proposed technical security controls (as depicted in fig. 4.3); however we have stated that organizational controls and implementation procedures (as described in table 4.2) should be also present.

Regarding the technical controls, it was pointed out as a recommendation that an additional internal firewall could be placed within the hub's intranet in order to separate the application servers from the databases, thus forming a "3-tier" architecture (with DMZ/web – application – database levels) for additional security, with the critical TSB databases placed at the third level. Finally, since special attention should be given on protecting the TSB keys, the use of an unidirectional gateway was suggested for this purpose.

We should also note that despite the fact that the risk assessment was based on a fictitious organization, we also based some of our assumptions and proposed security controls on cases of existing CAs. Interestingly, a common pattern was found in various cases of CA security breaches in the past: In most cases it was the poorly defined security procedures or employee malpractices that led to a security breach (Asghari, et al., 2013). In this aspect, experts also agreed that installing the appropriate physical and technical controls is essential, but the real challenge lies on defining, and most importantly implementing, proper organizational security procedures and promoting employee awareness.

A very important remark was made regarding the relation of the internal TSB security to the actors' systems. In the first section of chapter 4, the scope of the risk assessment was limited to the TSB system (and incoming communication), meaning that the internal security of CAs or actors' systems was their own responsibility. Although this is a reasonable assumption, it was pointed out during the validation process that it is very important for the TSB to be immediately notified when the certificate (considering the implementation of an enterprise PKI) of a particular entity expires, for instance in the case of an employee termination. The importance lies on the fact that when an entity is terminated from its organization, it should also refrain from using a TSB certificate, for obvious reasons. In other words, it should be made explicit within the TSB terms of use that every organization must be responsible for informing the local TSB hub in such cases and will be liable when it fails to do so. In a similar context, it was also pointed out that, at least initially, the TSB's reliability heavily depends on the internal security of local CAs, as a potential CA compromise can subsequently hinder the ability of the TSB to securely identify actors during the first steps of the initialization protocol.

Furthermore, with regard to the risk assessment process, even when considering the fact that an asset clustering has been performed, it might still seem that some assets were not examined in detail (or at all); however, this is not the case. To be more specific, the TSB application, a vital asset within the TSB architecture is not extensively examined in itself. However, it is widely analyzed in relation to other assets, when the *application* DID layer is considered. Similarly, server and other infrastructure components (eg. client computers or network components) are not extensively examined as standalone assets; instead we analyze the risks and implications with regard to other assets (i.e. critical data) when infrastructure components are compromised (eg. at the network or host DID layers). In other words, this is mostly a matter of risk statement formulation.

Finally, chapter 4 revolved around the internal security of each TSB hub individually. However, recent history has shown that the implementation of such internal security controls is not a panacea. In this aspect, it has been pointed out that it may still be the case that a hub is unable to resist a sophisticated attack, or collapse due to an internal system failure, particularly considering that the infrastructure security controls and software quality may not be mature enough, at least initially. The fact that the TSB consists of distributed hubs (peers), offers alternative possibilities for redundancy in a case of a hub's failure. Such a solution is going to be described in more details in section 5.2.

5.1.3.5 Usability

Although a TSB implementation, involving organizational and legal considerations and requirements, has been repeatedly stated to be out of this Thesis' scope, all experts agreed that probably the biggest challenges towards a successful TSB implementation are related to these issues. As a result, we consider it important to at least briefly describe some of these challenges regarding the usability of the TSB as an artifact.

First of all, although the TSB is considered to be independent of governmental consent (in contrast to CAs), the rules for its operations are still defined by both local and international trade regulations. In this aspect, compliance with these regulations is mandatory for a successful future TSB implementation. The establishment of TSB hubs through joint ventures with local organizations (ideally with actors involved in the international supply chain) could significantly facilitate compliance with local regulations and also increase the offline reliability of the TSB.

In addition, apart from establishing a well-defined TSB policy / use terms (as soon as the TSB hubs are organizationally materialized), it is also important that all relying entities are fully aware of this policy. For this reason, during the initialization protocol, actors receive an (electronic) copy of the policy, so that they are fully aware of what they can expect from the TSB (for instance in terms of real time support) and also what is required from them.

Furthermore, serious problems may rise if more than one organization wishes or claims to be the "official" TSB hub within a certain region (particularly in countries / regions with unstable political conditions). To deal with such an issue, *mutual agreements* between all TSB hubs should be established, so that a single, official TSB network can exist. In addition, the presence of TSB hubs distributed around the globe raises management

concerns on an organizational level and as a result governance mechanisms should be properly defined.

Finally, standardization of trust policies across different regions was also pointed out as a potential challenge. The TSB issues certificates to actors in a uniform format, but the identification of each actor is based on a local trust chain with different types of certificates. In this sense, the TSB should also play a role in establishing the same trust levels across different regions. Defining the rules for interpreting the local trust policies can therefore be a significant challenge.

5.2 Generalization and global deployment

Throughout this Thesis, we have channeled our focus on demonstrating how the TSB architecture could facilitate secure and efficient information exchange within a specific business context. In this aspect, we have limited our (geographic) scope to two regions, specifically the Netherlands and Malaysia. Nevertheless, the TSB's ultimate goal is to facilitate secure information exchange in a global scale. Obviously, we are well aware of the fact that a global TSB implementation cannot be achieved from one day to the next, particularly when considering the issues described in section 5.1.3.5. Still though, we believe that it can be done and figure 5.1 gives a visualization of our views for the future. For simplicity, only 8 interconnected TSB hubs are depicted; however this logic can be extended to involve more hubs in additional regions.

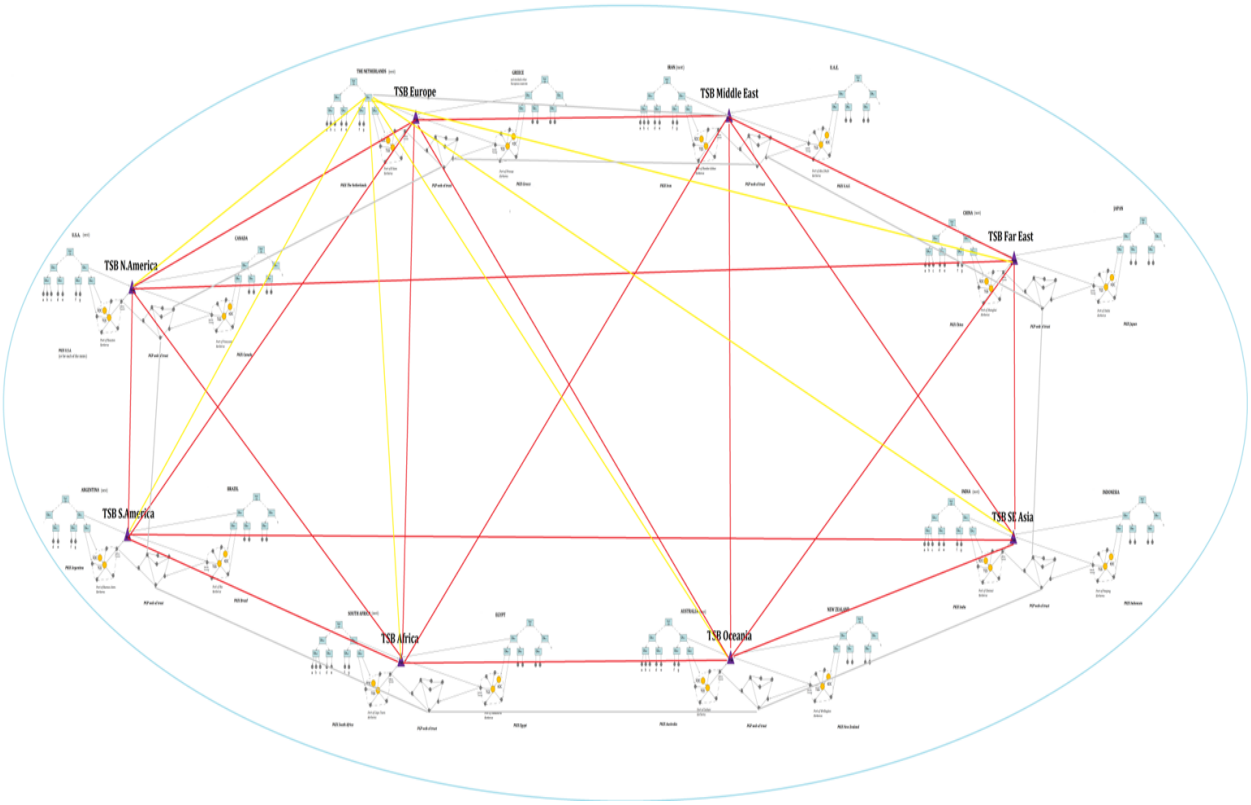

Figure 5.1: Global TSB deployment

To expand more on this, we could argue that the TSB can become a backbone of trust, much like the "Distributed Trusted Backbone" described in (Pruskasri, et al., 2013). First, the TSB can obviously handle the role of the registration system, although this is now distributed (as described in ch.3) instead of virtually centralized, in order to deal with the fact that a common CA between different regions does not exist. In addition, the TSB hubs can also play the role of country gateway systems. To begin with, the TSB hubs are already linked to the local chains of trust (eg local PKIs / e-ID systems) and we have also argued that actors already interact via the TSB hubs in order to communicate with each other. Nevertheless, this interaction is limited to the provision and verification of a global trusted ID. In order to solve the **complexity problem** in global data exchange, the role of the TSB can be extended, by forcing the international supply chain actors to exchange information via the TSB hubs, instead of directly communicating with each other. Assuming n supply chain actors globally and m TSB hubs (where m<<n), the number of communication links needed when actors interact via the TSB hubs falls from a number of order n^2 to a number of order m^2n, which is much more efficient (Pruskasri, et al., 2013). To sum up, the network of TSB hubs can play the role of *both* the registration system *and* the country gateway systems, thus eliminating the need of involving institutionalized organizations (such as the country gateway systems, which can pose bureaucratic and administrative burdens), as well as removing the assumption that a common CA exists between two different regions.

Another thing to consider when examining a global TSB deployment is that obtaining multiple certificates from the local CAs may only be a temporary necessity. Since the TSB is nested as a peer, certification is most needed in order to deal with the initial phase of distrust. In other words, after a successful number of experiences, the TSB hubs will be able to be considered as trusted PoRs by actors within the corresponding regions. In order to come to this point, however, the TSB must first obtain sufficient resources so that it can also act as a Registration Authority and accept actors even without local certification. In any case, we still acknowledge that by obtaining multiple certifications, the TSB gains additional credibility; our purpose was to indicate that given enough time, the TSB hubs could also become independent of local CAs and perform RA functions as well.

Resilience

The fact that the TSB hubs can be regarded as a backbone of trust raises the concern that they can be also considered as **multiple single points of failure** (MSPFs), for instance in case of a sophisticated denial of service (DoS) attack against them (Daskapan, et al., 2004). Although the distributed TSB concept as described in section 3.2 implies that in case of a hub failure the rest of the TSB network can still provide its services to the other regions, the inability of actors in this region to communicate with their partners and vice versa is still a major concern that cannot be overlooked. In chapter 4 we have described conventional means for the security of the TSB hubs, which aims at protecting the hubs from common attacks or internal errors. However, as history has shown, with the breaches of various CAs (Asghari, et al., 2013), sometimes an unidentified attack cannot be repelled, thus resulting in the hub's failure. In such cases, a "back-up" plan should be in place to guarantee that the TSB operations are not interrupted. Redundancy through additional dedicated hardware within each hub could be a solution; however it requires a significant budget (which may not be available for the TSB, at least initially) and it is also inefficient, as redundant systems only

become operational when the main system is down (Daskapan, et al., 2006). In this sense, it would be much more efficient if these systems could be also used in the remaining time. Therefore, *resource sharing* can be considered as a viable and more efficient alternative.

Given the TSB context, the protocol set Medusa, described by (Daskapan, et al., 2006), can provide an adaptive distributed defense system that can enable perpetual availability for the TSB system, allowing the hubs to resist failures. The basic premise is that when a hub fails, the trust services can be provided by another hub until the former becomes available again. The distributed TSB concept is of particular importance for two reasons. First, in a case of attack, trust can easily "hop" to any collaborating hub (Daskapan, et al., 2004). Second, by anchoring each hub in a given region through obtaining multiple certifications from local CAs, the first phase of the Medusa protocol (bootstrapping phase) is already dealt with: The TSB hubs are already trusted by the supply chain actors. In this sense the group of "leaders" which will share resources between each other, as well as the relying peers, is already established.

In the second phase of the Medusa protocol, the preparation phase, the TSB hubs take measures of precaution in order to be able cope with future failures (Daskapan, et al., 2006). This involves the selection and distribution of a unique "trust token", which can be seen as the sign of authority for every hub (leader). We propose that the private key of each hub is an ideal trust token for two reasons. First, it is unique and only known to each hub and can be therefore regarded as the definite sign of authority for each leader. Second, this private key is essential for performing key functions (eg. certificate signing). In this sense, when a hub fails, it is important for its successor to possess this private key, so that it can be trusted by the relying peers and perform the necessary functions. To sum up, in this phase, all the private keys of the TSB hubs are split in pieces and distributed to other hubs, for instance using an algorithm like Shamir's (Daskapan, et al., 2006). In addition, we propose that in this phase, each hub's successor in case of a failure is pointed out, by taking into account the geographic proximity between hubs and political/trade conditions between regions. Finally, since both the infrastructure and the execution environment (i.e the TSB application) is assumed to be common for all hubs, the TSB services can be carried on by the successor without any further difficulties. One thing that needs to be taken into consideration, however, is that the certificates of actors within a particular region are only held in the repository of the corresponding hub; in this sense, we could argue that every hub should periodically forward the contents of its repository to its successor, so that they can also be utilized in case of a potential failure.

When a TSB hub suffers an attack that cannot be dealt with by its innate security system, for instance due to a persevering DoS attack or any other random system failure, and the other hubs determine that the suffering hub cannot reply to requests in a timely manner (according to phase 3 of the Medusa protocol), the trust token of the suffering hub can be reconstructed (phase 4). In order to do so, the successor needs to collect a majority of the token's secret pieces from the other TSB hubs (Daskapan, et al., 2006). When the private key is reconstructed, the successor TSB hub can continue to provide the trust services to the supply chain actors within the region of the collapsed hub, until the latter becomes available again. With all this being said, it is evident that the Medusa protocol can

be regarded as a very efficient means of redundancy for the TSB system in case of a hub's failure, as it particularly suits the distributed TSB concept.

5.3 Conclusion

In this chapter we have discussed to which extent the TSB solution can be validated and generalized, thus addressing the fifth sub-question. Regarding the validation process, a major point was that the TSB solution could be validated only in theory by gathering expert opinions and not through testing in a real environment, due to a lack of time and resources. As a consequence, we were fully aware that the validation results would be weak per se. Nevertheless, we were able to gather invaluable feedback, particularly regarding the significance, technical feasibility and flexibility of the TSB solution (which was positively received) and was, after all, the main focus of this Thesis. We were also able to draw conclusions regarding the potential usability.

Finally, although our focus throughout this Thesis was to show the effectiveness of the TSB in a given case which included actors in two regions, we considered it important to also give our vision for a generalized TSB solution and a global deployment. In the same context, we also provided some further details on how the TSB hubs can actually achieve perpetual availability through the Medusa protocol set.

CHAPTER 6: Conclusions

6.1 Reflections and contribution

In chapter 1 we have described the generic trust domains problem as the main research problem under consideration: "*There exists no universal trust model to efficiently provide a secure communications path across different trust domains worldwide".* In this aspect, we defined our objective as designing an alternative solution, namely the Trust Service Broker architecture, to enable secure and efficient information exchange between information infrastructures that reside across different geopolitical domains, independent from the consent of governmental organizations. By looking through a specific business perspective, we narrowed down the scope of our research and the main research question of this Thesis became: "***What are the components, communication processes, functions and internal security controls of the TSB architecture so that organizations within the international supply chain can efficiently exchange information and resources?"***

In order to answer the main research question, we first focused on the processes (presented in figure 2.2) and information flows (presented in figures 2.3 to 2.5) between the international supply chain partners, particularly considering the implications of the trust domains problem within this specific business context. In this sense, we discussed the problems that the international supply chain actors could face when exchanging sensitive information, which mainly regarded the difficulty of establishing a trusted global ID. The first sub-question was therefore addressed.

In relation to these problems, we have also defined the main design requirements of the TSB architecture in section 2.3, which were summarized in table 2.2 and further analyzed in section 3.1, thereby addressing the second sub-question.

The rest of chapter 3 focused on presenting the constituents of the TSB architecture, thus addressing the third sub-question. We began by describing the distributed TSB concept in section 3.2 and the components of the TSB architecture in section 3.3, with an overview of these components being provided in figure 3.3. Subsequently, we presented the most important communication processes and functions of the TSB architecture (in the form of the initialization protocol shown in figure 3.7 and a specific communications scenario shown in figure 3.8), in order to show how the TSB components could be utilized in order to provide a global trusted ID and facilitate secure information exchange between the international supply chain actors.

We had also argued that in order to be able to do so, the TSB should be secure as a system itself and therefore meet certain security requirements. For this reason and to answer the fourth sub-question, a security risk assessment was performed in chapter 4, in order to establish the TSB's internal security controls. The most important results of the risk assessment were provided in table 4.2 and an overview of the TSB system with the proposed security controls was presented in figure 4.3.

Finally, in chapter 5 together with the validation process we have also discussed various legal and organizational concerns that need to be addressed in order to ensure a successful implementation, as well as our view for a potential global TSB deployment, thereby addressing the fifth sub-question.

It should be evident that our research has both a scientific and practical significance and can provide valuable input for the academic and business fields. Building on the work of (Daskapan, et al., 2004), we have further refined the TSB concept into a detailed TSB architecture and we have thus made an extra step towards dealing with the trust domains problem. In addition, our work provides the basis for a solution of an important business problem, as we have aligned our scope to the international supply chain environment. Apparently though, further research and, most importantly, testing in a real-world environment is essential before the TSB architecture can be applied in practice, but still, the foundations have been established. Such limitations, as well as the need for future research, are discussed in the next section.

6.2 Limitations and future work

As a general remark, and looking from a broader perspective, it could be quite utopic to suggest that "cracking" the problem of global distrust would mean that organizations in *all* regions worldwide will be able to share resources securely with each other. A main reason for this is that some countries may not be advanced enough technologically (by means of infrastructure) to support a TSB service. In addition, there are also countries that limit, or even prohibit communication to the outside world (an example being North Korea). Hence, the proposed architecture can only be a solution for organizations operating in politically open (meaning, in principle, that there are no trade barriers) and technologically advanced countries.

With regard to the need for future work, this essentially falls down to two main points. First, deployment and testing in a real lab is necessary in order to accurately determine potential technical and security issues. And second, some theoretical aspects also need further research before we can consider a TSB implementation.

In relation to the first point, although we have argued that the TSB architecture is technically viable, validation was only done from a theoretical perspective. We have stated that a working demonstration of the TSB architecture in a global scale would require time and resources that are out of our reach and was therefore out of scope. Nevertheless, as with any new technology, testing in a real-world environment is essential in order to determine its potential and the chances for adoption. In this sense, we feel that an environment similar to the Living Labs of the CASSANDRA project could be an ideal starting "testing ground" for the TSB.

Regarding the second point, we have already argued that the absence of an established TSB hub, significantly limits the conclusions that can be drawn out of the security risk assessment we have performed. While still being a useful guide for the future, it is

imperative that a more thorough assessment is performed upon the organizational establishment of the TSB.

In the same context, although the TSB architecture is a technically feasible solution, we have identified various organizational and legal challenges, which also need to be extensively researched before commercialization can be considered.

Bibliography

Adams, C. & Lloyd, S., 2002. *Understanding PKI: Concepts, Standards, and Deployment Considerations.* 2nd ed. :: Addison-Wesley Professional.

Asghari, H., van Eeten, M. J., Arnbak, A. M. & van Eijk, N. A., 2013. *Security Economics in the HTTPS Value Chain,* Delft: Netherlands.

CASSANDRA, 29-04-2012. *Intermediate Report Asia-Europe p. 28-36,* EU: Seventh Framework Programme.

Chiu, R.-K. & Chen, J. C., 2005. A generic service model for secure data interchange. *Industrial Management & Data Systems,* 105(5), pp. 662-681.

Choudhury, S., Bhatnagar, K. & Haque, W., 2002. *Public Key Infrastructure Implementation and Design.* 1st ed. New York: M&T Books.

Daskapan, S., 2005. MEDUSA: Survivable information security in critical infrastructures.

Daskapan, S., 2012. *IT Security Risk Management: From Risk to Security.* Delft: Lecture slides.

Daskapan, S., 2012. *Security and Reliability for E-business.* Delft: s.n.

Daskapan, S., Costa, A. C., Vree, W. G. & Eldin, A. A., 2004. *Virtual Trust in Distributed Systems.* Berlin: Springer.

Daskapan, S., Vree, W. G. & Sol, H. G., 2004. *Building a Distributed Security Defence System.* Delft: IEEE.

Daskapan, S., Vree, W. G. & Wagenaar, R. W., 2006. Emergent information security in critical infrastructures. *Int. J. Critical Infrastructures,* 2(2/3), pp. 247-260.

Deane, J. K., Ragsdale, C. T., Rakes, T. R. & Rees, L. P., 2009. Managing supply chain risk and disruption from IT security incidents. *Operations Management Research,* 1(2), pp. 4-12.

El-Ashqar, A. A., Mageed, T. A. & Fahmy, A. A., 2012. Taxonomy of Public Key Infrastructure. *Journal of Applied Sciences Research,* 8(7), pp. 3656-3663.

Eshuis, R., 2006. Symbolic Model Checking of UML Activity Diagrams. *ACM Transactions on Software Engineering and Methodology,* 15(1), pp. 1-38.

GS1, 2012. *GS1 Malaysia.* [Online]
Available at: http://www.gs1my.org/events_details.aspx?eventID=26dfbf89-c79f-4f7d-91a4-c631c848a0e4
[Accessed March 2013].

Gutmann, P., 2002. *PKI: It's Not Dead, Just Resting.* IEEE: Computer Society.

Henderson, J. C. & Venkatraman, H., 1999. Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal,* 38(2), p. 472.

Hesketh, D., 2010. Weakness in the supply chain: who packed the box?. *World Customs Journal,* 4(2), pp. 3-20.

Hevner, A. R., March, S. T., Park, J. & Ram, S., 2004. Design Science in Information Systems Research. *MIS Quarterly,* 28(1), pp. 75-105.

Hofman, W., 2011. *Applying semantic web technology for interoperability in freight logistics.* Munich, e-Freight event.

Hofman, W., 2011. *Supply Chain Visibility with Linked Open Data for Supply Chain Risk Analysis.* Delft, 1st Workshop on IT Innovations Enabling Seamless and Secure Supply Chains.

Hofman, W. & Bruijning, J., 2008. *Naar een federatief stelsel van identiteit en autorisatie.* Delft, TNO.

Hulstijn, J., Overbeek, S., Aldewereld, H. & Christiaanse, R., 2012. *Integrity of Supply Chain Visibility: Linking Information to the Physical World.* CAiSE 2012 Workshops LNBIP 112, pp.351-365, Sringer-Verlag Berlin Heidelberg.

IBM, 2013. *Info center.* [Online]
Available at:
http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=%2Fcom.ibm.itame2.doc_5.1%2Fss7aumst18.htm
[Accessed March 2013].

Iivari, J., 2007. A Paradigmatic Analysis of Information Systems As a Design Science. *Scandinavian Journal of Information Systems,* 19(2), p. Article 5.

Kedia, L. B. & Lahiri, S., 2007. International outsourcing of services: A partnership model. *Journal of International Management,* Volume 13, pp. 22-37.

Kolluru, R. & Meredith, P. H., 2001. Security and trust management in supply chains. *Information Management and Computer Security,* 9(-), pp. 233-236.

Lioy, A., Marian, M., Moltchanova, N. & Pala, M., 2006. PKI past, present and future. *International Journal of Information Security,* 1(5), pp. 18-29.

Lopez Millan, G., Perez, M. G., Martinez Perez, G. & Gomez, A. F., 2010. PKI-based trust management in inter-domain scenarios. *Computers & Security,* Volume 29, pp. 278-290.

Lopez, J. et al., 2005. Specification and design of advanced authentication and authorization services. *Computer Standards and Interfaces,* 27(2005), pp. 467-478.

Lopez, J., Opplinger, R. & Pernul, G., 2005. Why have public key infrastructures failed so far?. *Internet Research,* 15(5), pp. 544-556.

Microsoft, 2006. *The Security Risk Management Guide.* San Francisco: Microsoft.

NIST, 2009. *Recommended security controls for federal information systems and organizations,* Gaithersburg: U.S. Department of Commerce.

NIST, 2013. *National Vulnerability Database.* [Online]
Available at: http://nvd.nist.gov/
[Accessed June 2013].

Oosterhout, M. v., 2008. 'Appendix A: Organizations and flows in the network', in 'Port inter-organizational information systems: capabilities to service global supply chains'. *Foundations and Trends in Technology, Information and Operations Management,* 2(2-3), pp. 81-241.

Overbeek, S. et al., 2011. *A Web-Based Data Pipeline for Compliance in International Trade.* Delft: Paper for WITNESS.

Pala, M. & Smith, S. W., 2010. Finding the PKI needles in the Internet haystack. *Journal of Computer Security,* 2010(18), pp. 397-420.

Peffers, K., Tuunanen, T., Rothenberger, M. A. & Chatterjee, S., 2008. A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems,* 24(3), pp. 45-77.

Pruksasri, P., Berg, J. v. d. & Hofman, W., 2012. *Three Protocols for securing the Data Pipeline of the International Supply Chain.* Delft, IADIS International Conference e-Commerce.

Pruksasri, P., Berg, J. v. d. & Keretho, S., 2011. *Accountability in single window systems using an internal certificate authority - A case study on Thailand's national single window system.* Rome, IADIS Multiconference on Computer Science and Information Systems.

Pruskasri, P., Berg, J. v. d., Hofman, W. & Daskapan, S., 2013. *Multi-Level Access Control in the Data Pipeline of the International Supply Chain System,* Delft: TUDelft.

Qing-hai, B., 2012. *Comparative Research on Two Kinds of Certification Systems of the Public Key Infrastructure (PKI) and the Identity Based Encryption (IBE).* Cross Strait Quad-Regional Radio Science and Wireless Technology Conference, IEEE.

rfc4210, 2005. *Internet X.509 PKI Certificate Management Protocol (CMP).* Standards Track: Network Working Group.

rfc5755, 2010. *An Internet Attribute Certificate Profile for Authorization.* [Online]
Available at: http://www.rfc-base.org/rfc-5755.html

Schneier, B., 1996. *Applied Cryptography.* 2nd ed. NJ: John Wiley & Sons, Inc..

Shankar, V., Urban, G. L. & Sultan, F., 2002. Online trust: a stakeholder perspective, concepts, implications, and future directions.

Sharifnia, M., Iranmehr, A. & Doroodchi, M., 2009. *Development of trust model for e-supply chain management applications.* Izmir, European and Mediterranean Conference on Information Systems.

Smith, G. E., Watson, K. J., Baker, W. H. & Pokorski, J. A., 2007. A critical balance: collaboration and security in the IT-enabled supply chain. *International Journal of Production Research,* 45(11), pp. 2595-2613.

SQA, 2009. *SQA: Network Infrastructure 2: Planning and Maintenance.* [Online] Available at: http://www.sqa.org.uk/e-learning/NetInf205CD/page_27.htm [Accessed April 2013].

Stijn, E. v. et al., 2011. *Single Windows and Supply Chains in the Next Decade: The Data Pipeline.* Global Trade Facilitation Conference, s.n.

Stijn, E. v., Klievink, B. & Tan, Y.-H., 2011. Innovative ICT solutions for monitoring and facilitating international trade. *Network Industries Quarterly,* 13(3), pp. 26-29.

Tanenbaum, A. S. & Wetherall, D. J., 2011. *Computer Networks.* 5th ed. .: Prentice Hall.

Tan, Y.-H., Bjorn-Andersen, N., Klein, S. & Rukanova, B., 2011. *Accelerating Global Supply Chains with IT-Innovation: ITAIDE Tools and Methods.* Berlin Heidelberg: Springer.

Xiong, K., 2012. *The Performance of Public Key-Based Authentication Protocols,* Berlin: Springer.

Xu, P., 2013. Information on Risks and Prevention of the Supply Chain in E-commerce Environment. *Advanced Materials Research,* 605-607(1), pp. 493-496.

Appendix 1A: Boundaries of the TSB architecture design

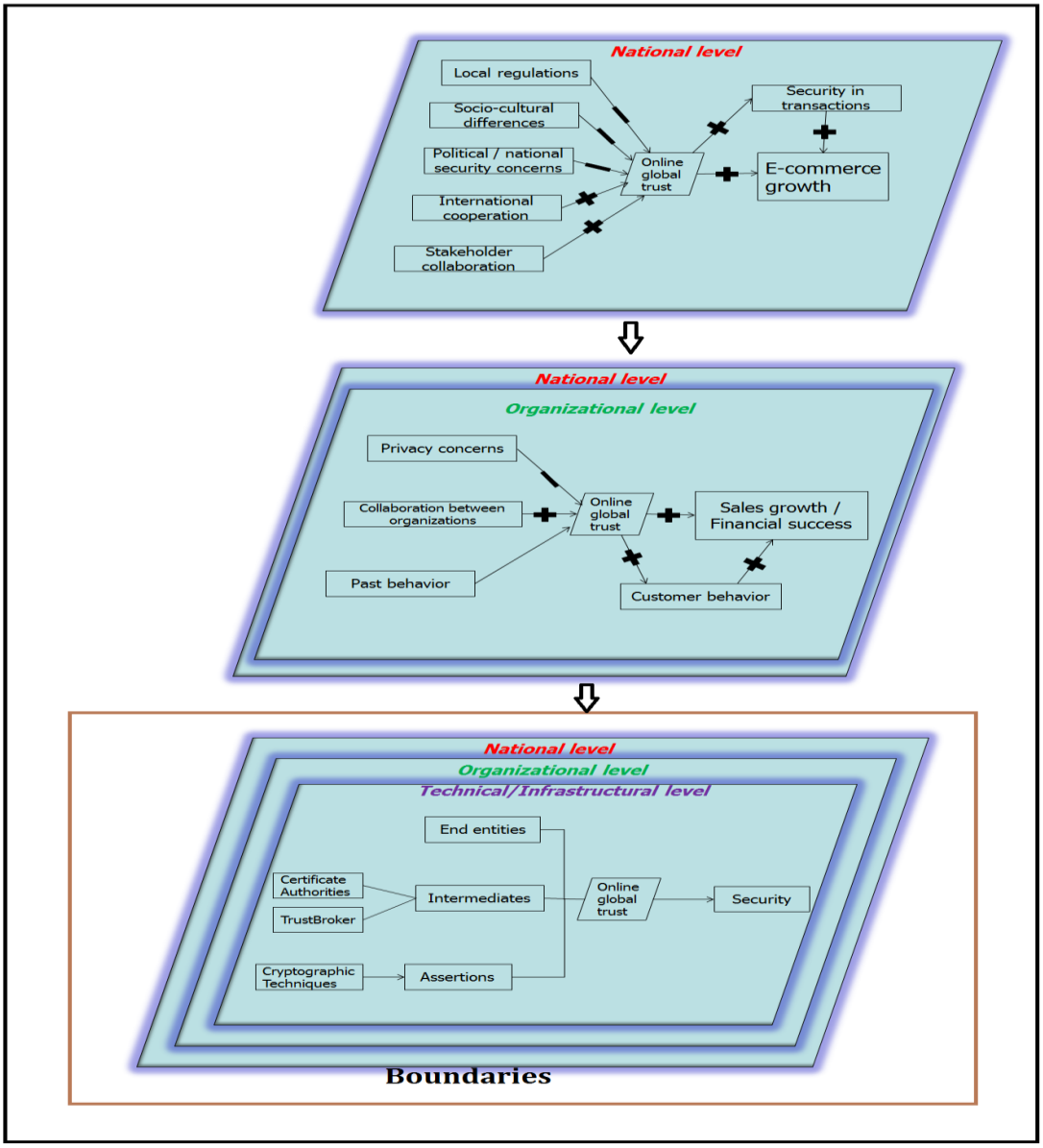

Figure 1A.1: TSB design boundaries

Appendix 1B: TSB conceptual model

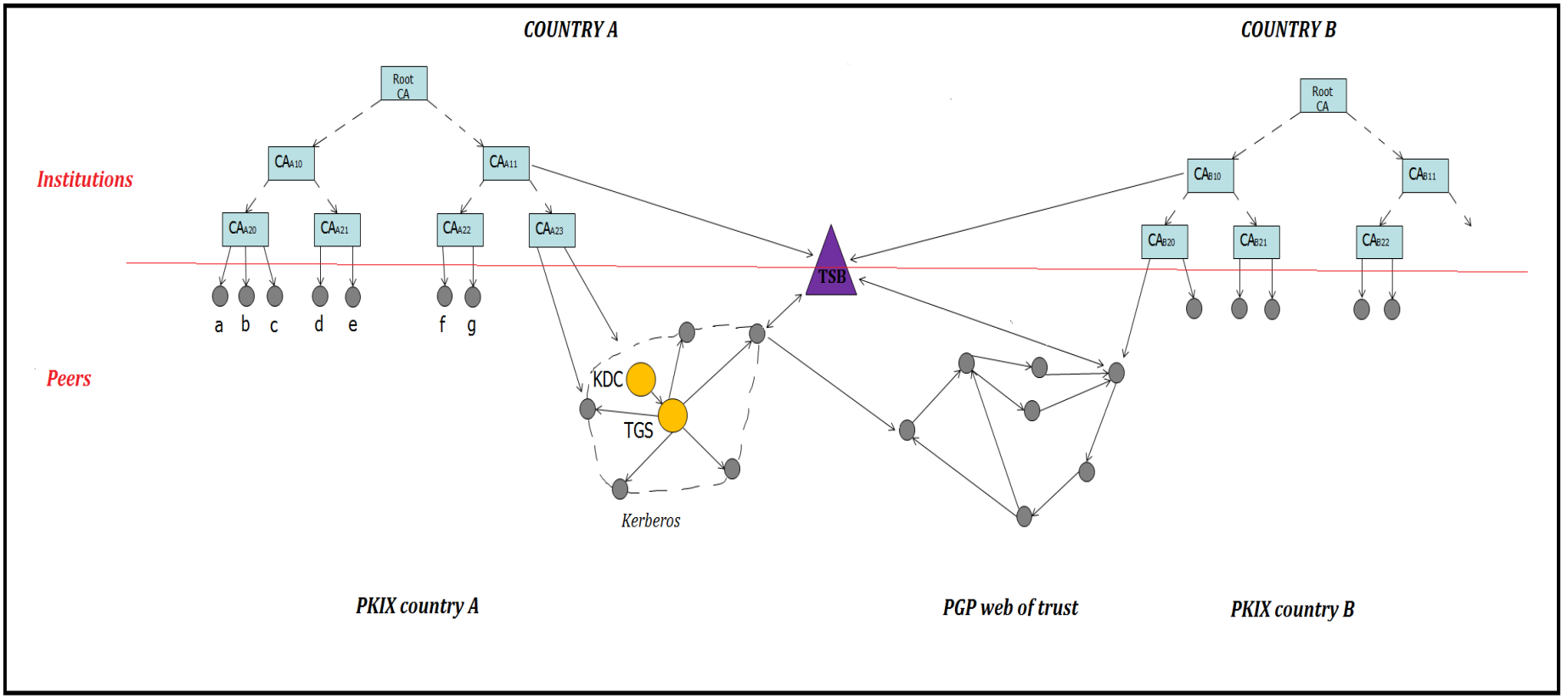

Figure 1B.1: TSB conceptual model. Source: (Daskapan, 2005)

Appendix 1C: High-level stakeholder description

The fact that the problem of global (dis)trust expands on multiple levels implies that numerous parties are affected and therefore have interests in the Trust Service Broker solution. The most important blocks of stakeholders associated with the TSB, along with their views are described in this section.

Since the problem of global distrust obviously has implications on a national level, governments and associated agencies clearly have interests on the TSB project. From a broader perspective, an efficient TSB solution can facilitate the growth of domestic companies which conduct business internationally, particularly those engaging in e-commerce activities. In this sense, the TSB can be viewed by the authorities as a means to further stimulate the economy of the country. Security concerns and more specifically the issue of online distrust is an important inhibitor regarding e-commerce growth in developing countries. On the other hand, however, due to political reasons some governments may be unwilling to establish bridges with certain countries worldwide. Since most local Certificate Authorities are often related to a government agency, they might be unwilling to provide certificates to a TSB nested in a particular foreign country due to such political reasons. In this aspect, considering a global deployment of the TSB service, all these implications on a national level must be taken into serious consideration. Nevertheless, since the TSB has the objective of being independent from the consent of governmental authorities (as it does not submit itself to any institution), the power of governmental agencies can be considered limited with regard to this aspect.

As already discussed, the benefits of the TSB development will be mainly reaped by organizations conducting business on a global scale, such actors within the international supply chain. Since trust is a major concern in online security, particularly when considering different domains, for instance countries, a global TSB establishment can provide considerable advantages to firms which choose to make use of it. Suppliers, distributors and retailers can obtain the answer to several questions that may currently trouble them: “Is a specific firm trustworthy for online collaboration?” “Is the online information reliable and consistent with offline information?” “How confidential is the information sharing?” and most prominently “Are we certain that our transacting partner is who he actually claims to be?” In this sense, such organizations can be viewed as proponents for the design and establishment of a global TSB service in the future. (Shankar, et al., 2002). For the specific logistics case where the effectiveness of the TSB architecture will be demonstrated, organizations interested in the TSB solution span across the international supply chain communities. A more detailed overview of these organizations was presented in chapter 2.

Apart from organizations, individuals may also engage in sharing information and resources online. For instance, customers of such e-businesses must also be confident that their transactions will be securely completed. In this sense, the TSB can also be regarded as the solution to such problems, interconnecting entities not only across different countries, but also across different trust domains in general (for instance a peer nested in a PGP web of trust with an organization nested in a PKI domain).

Due to the nature of the service provided by the TSB, Certificate Authorities will be needed to provide the TSB with the essential certifications, which will be further used to interconnect entities from different trust domains. Again, due to local regulations or political issues, some may be unwilling to issue certificates to TSBs nested for instance in "hostile" countries. In this aspect, before establishing the selection of countries to host the TSBs worldwide must also take this issue into account. In any case, the interest of CAs can be considered limited, since in essence the TSB is just another customer to sell their certificates.

Finally, an organization (for example a central actor in the international supply chain for our case) possessing the necessary resources will handle the implementation of the TSB on a global scale.

Table 1C.1 summarizes the main blocks of stakeholders, giving an indication on their interest towards the TSB (high or low), their attitude (positive or negative) and their power in terms of their ability to exert influence (high or low).

STAKEHOLDERS	Interest	Attitude	Power
Governmental agencies	+ / -	+ / -	-
Organizations conducting business worldwide*	+	+	+
Customers	+	+	-
Certificate Authorities	-	+ / -	+
TSB service provider	+	+	+

Table1C.1: Stakeholder Overview

*a detailed overview of organizations involved in the logistics case is provided in chapter 2

Appendix 2A: The international supply chain environment and ICT innovations

In contemporary times, the globalization of the economy has changed the way business is conducted around the world. It is most often the case that goods will travel throughout the globe from suppliers to transporters, buyers and sellers across the international supply chain, before they reach their final destination. The decline of vertically integrated organizations together with an increasing trend for outsourcing has resulted in competition being seen as between supply chains rather than between firms (Smith, et al., 2007).

Advances in Information Technology have facilitated the integration of information flows, thus increasing collaboration across supply chains. A primary driver for this integration is the recognition that supply chains achieve maximum efficiency for all members when sharing information for coordinated decision making. As the need for collaboration increases, so does the need for integration and the ability to process and analyze information which is shared among the supply chain partners (Smith, et al., 2007). In other words, by enabling organizations to capture, process, store and exchange information over vast geographical distances and also in a timely manner, IT has become an indispensable tool for supply chain collaboration. In this sense, the need for strategic integration between business processes and IT as described by (Henderson & Venkatraman, 1999) is also evident when considering the supply chain as a whole. IT alignment within a supply chain is therefore as one of the most efficient ways to support the development of stronger, more collaborative relationships within a business network.

The types of information shared among partners in order to facilitate collaborative undertakings have been described by various researchers. Partner Interface Processes (PIPs), as described by (Chiu & Chen, 2005), specify various kinds of system-to-system procedures for each trading activity. They are organized into seven clusters of core business processes, which are further broken down into segments. As such, information exchange among partners is related to:

1) Partner product and service review
2) Product information
3) Order management
4) Inventory Management
5) Marketing Information management
6) Service and report
7) Manufacturing

An alternative approach is presented in the framework by (Kolluru & Meredith, 2001), where the degree of integration among supply chain partners dictates the type of information which is shared. At the lowest level of integration, information sharing is limited to rudimentary information requirements, such as inventory levels, order status, sales data capacity and schedules for production and delivery. In contrast, supply chains exhibiting high levels of integration operate at a strategic level of collaboration. As such, the types of

information shared exceed rudimentary requirements and also include process, customer, supplier, competitive and marketing information.

So far we have discussed the role of information sharing merely among business partners within the international supply chain. Nevertheless, information related to supply chain operations is also crucial for controlling purposes. It is a fact that the movement of goods across borders is highly regulated, as governments try to deal with issues such as fraud, safety and smuggling. As such, businesses are obliged to submit a vast amount of data and, in addition, Customs and other agencies perform physical inspections on goods. According to the Asia-Pacific Economic Cooperation Business Advisory Council, 40 documents meeting the rules and regulations of international trade and transport are required in each international trade transaction (Stijn, et al., 2011). As a result, supply chain partners must also share information related to their operations with certain authorities. In this context, (Oosterhout, 2008) described a multi-layer approach for the supply chain, with a Governance Layer being on top of the Transaction and Logistics Layers, while also making the distinction between physical, information and financial flows along the supply chain (Hesketh, 2010). This non-linear, three-layer approach of the supply chain is presented in figure 2A.1.

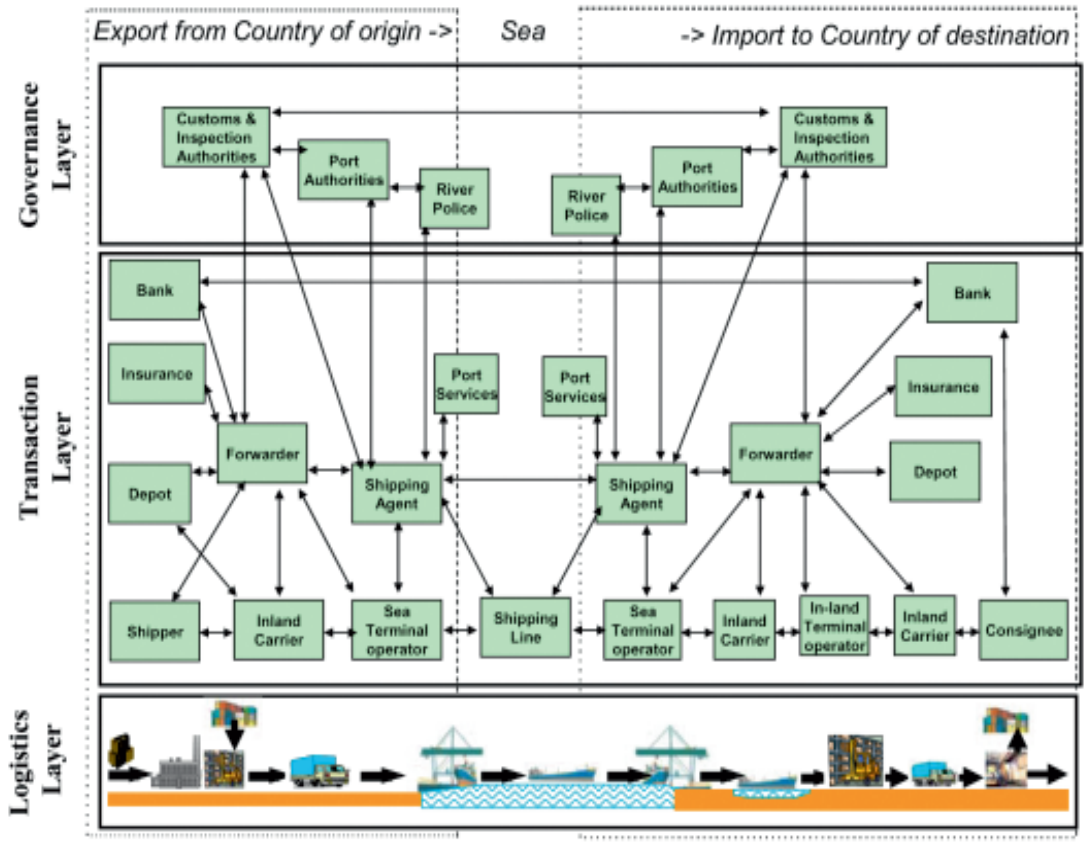

Figure 2A.1: Three-layer supply chain. Source: (Hesketh, 2010), adapted from (Oosterhout, 2008)

2A.1 ICT innovations for international trade: Enhancing the supply chain visibility

It has already been discussed that the movement of goods worldwide is highly regulated. However, at the same time authorities strive to facilitate trade by reducing administrative burdens and increasing competitiveness, which seems to be in contradiction to the need for control (Stijn, et al., 2011). In this aspect, the role of ICT in reducing such administrative burdens is prominent. Many efforts and suggestions have already been made to switch from a paper-based document exchange regime (posing heavy administrative issues) to a paperless environment, by utilizing innovative ICT solutions, such as single window systems (Pruksasri, et al., 2011). Although the implementation of such information systems – at least initially – was uncoordinated throughout the EU thus posing some interoperability issues, the basic premise is that innovative ICT solutions can improve information sharing both within the supply chain and, most importantly, between business and government. Hence, ICT innovation can be regarded as a means to achieve (Stijn, et al., 2011):

- Efficiency improvement (for example reducing the administrative burdens)
- Effectiveness improvement (for example coordinated inspections)
- Strategic changes (for example risk-based governance)

Apart from the motivation to facilitate trade by reducing administrative burdens, it is also apparent that it is infeasible to physically inspect all goods, due to the massive amount of international trade transactions. For these reasons, customs generally use a risk-based approach in order to determine the selection of freights for inspection. These risk assessments require reliable data regarding the transportation movements and container contents (Hulstijn, et al., 2012). The current regulatory process for international trade is depicted in figure 2A.2.

However, data in the supply chain can be inaccurate and rarely administered, operated or managed in a uniform way. In addition, it is often subject to varying degrees of integrity, while at the same time the movement of goods might not be visible to the buyer and seller. (Hesketh, 2010) also argues that there is ample evidence that goods are not properly described or dispatched for both transport and regulatory purposes, thus creating risks to the buyer, carriers and to the society as a whole. Since goods can move along the supply chain as part of contracts with varying degrees of integrity in terms of transport or carriers, untrustworthy operators can exploit these deficiencies and defraud about $20 billion annually. (Hesketh, 2010)

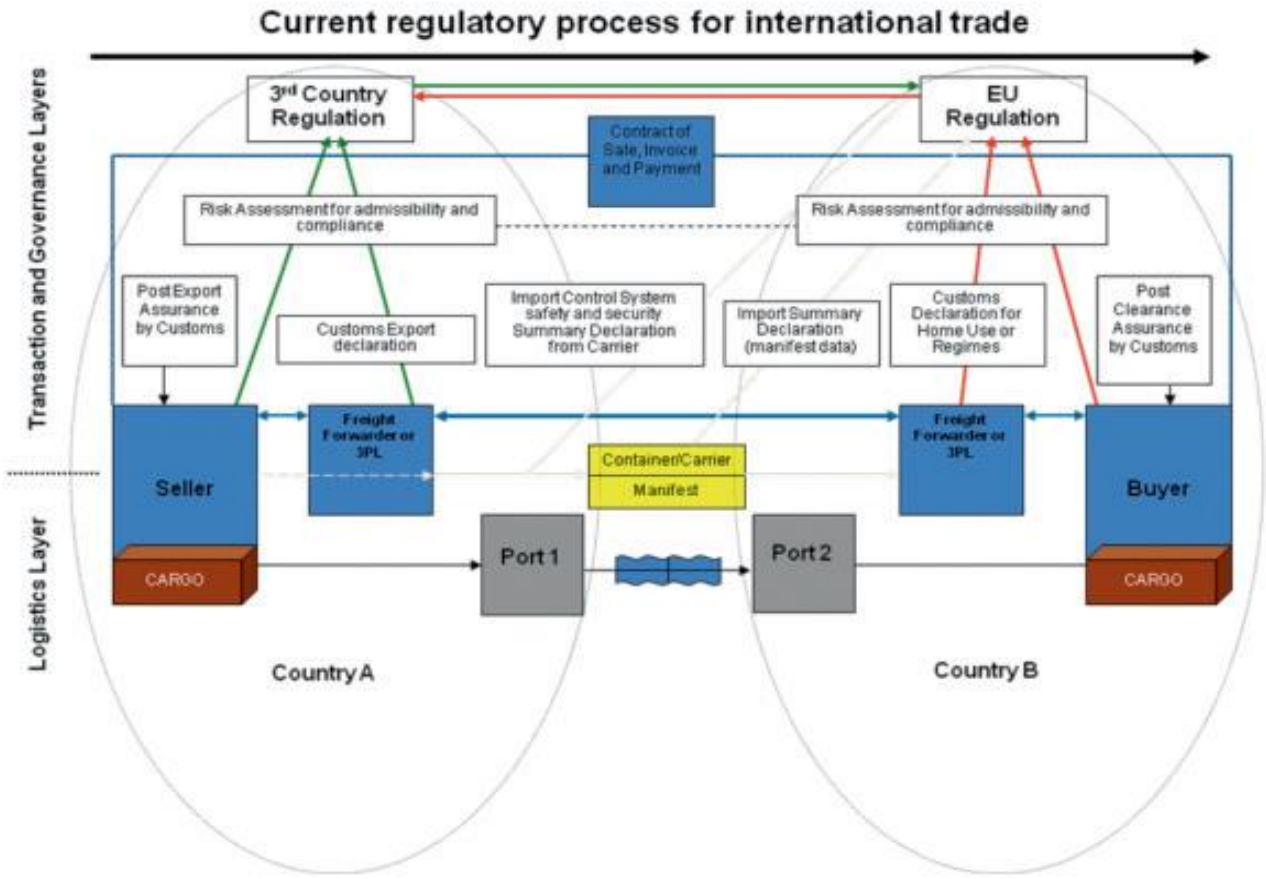

Figure 2A.2: Regulatory process for international trade. Source: (Hesketh, 2010)

Apparently, the supply chain is organized in such a way that the data cannot always be considered reliable. One way to deal with this issue is to enhance the transparency and visibility in the supply chain, which can be achieved through ICT innovations (Hulstijn, et al., 2012) (Stijn, et al., 2011). The ITAIDE project, running from 2006 to 2010 aimed to enhance the supply chain visibility by utilizing ICT innovations, for instance web-services based on open standards. The fundamental principles behind the ITAIDE approach are piggy-backing and data pull. Piggy-backing refers to the re-use of existing business data for government control purposes. As such, interested governments can pull information from the business systems of companies when needed, instead of businesses directly submitting information to authorities, thus making the acquisition of real-time data a possibility (Tan, et al., 2011).

Building on these principles, a more specific approach to enhance supply chain visibility is the ***virtual data pipeline***, developed in the CASSANDRA research project (running from 2011 to 2013). In essence, the data pipeline is a data sharing architecture based on Linked Open Data, which is the most commonly known application of the semantic web (Hofman, 2011) (Hulstijn, et al., 2012). A perquisite for implementing a global data pipeline is to describe data in a standardized, uniform way. As such, semantics are represented as an ontology in order to provide access for all authorities and enterprises involved in the supply chain. In this aspect, (Hofman, 2011) also argues that “applying a semantic web technology

such as Web Ontology Language (OWL) for specification of semantics instead of UML class diagrams enables referencing to centrally maintained models with their specific rules".

A primary principle underlying the data pipeline concept is that only the original trade data – which are provided by the consignor – are shared and can be subsequently used by authorized parties in the trade network. Essentially, all actors participating in the supply chain provide data that can be relevant to other parties (both within the trade network and for regulatory purposes) in a shared information space (Stijn, et al., 2011). As in the ITAIDE project, the piggybacking and data pull principles are also applied within the data pipeline concept. A key advantage for authorities resulting from these principles is that they can obtain the original data directly from the source, without being altered by someone else. (Stijn, et al., 2011)

Information which is shared among parties within the data pipeline can describe:

- Transactional data
- Physical data
- Commercial risk management data

In addition, a distinction is made between the data related to goods and people and data related to the carriage itself. In this sense, different types of data are shared with different parties, for different purposes. Finally, it is important to also note that, from a legal perspective, the parties with which the data may be exchanged are determined by legislation at the national, EU or federal level, depending on the import destination (Stijn, et al., 2011).

Figure 2A.3, presented below, provides an overview of what kind of shipment data is exchanged in the supply chain through the data pipeline (Overbeek, et al., 2011).

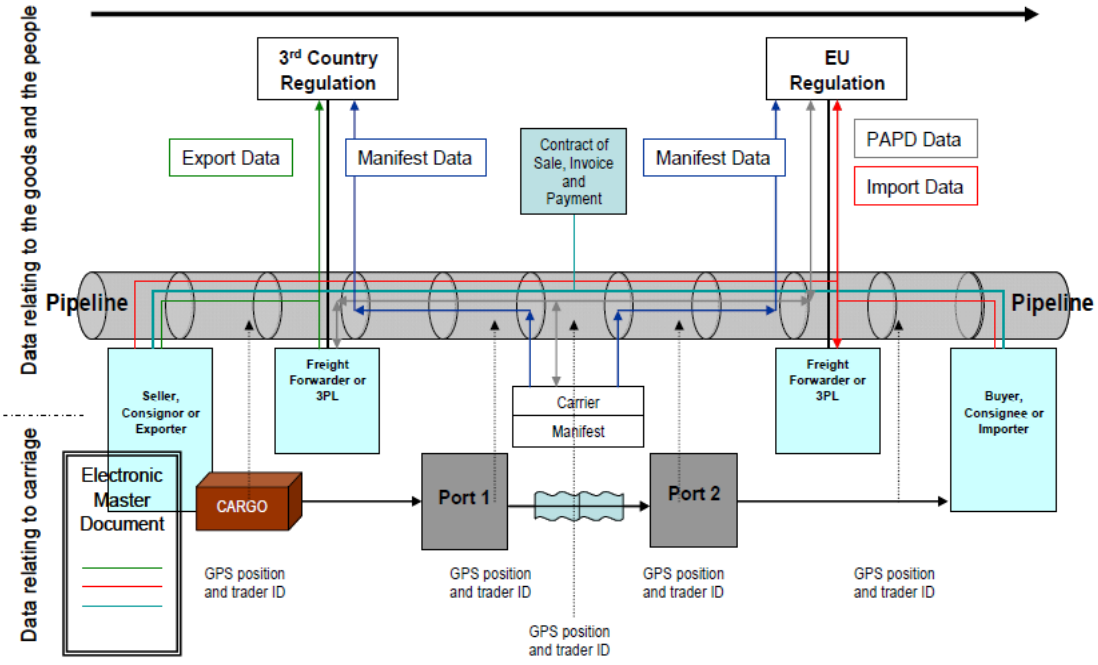

Figure 2A.3: Seamless integrated data pipeline. Source: (Overbeek, et al., 2011) adapted from (Hesketh, 2010)

2A.2 Stakeholders

A vast number of inter-organizational and international stakeholders are involved both in using and enabling the data pipeline. Since partners from all around the globe are linked up to a single pipeline, there is consequently high diversity among them. This diversity can be described in social, cultural, legislative and political terms and can often result in different or sometimes even conflicting interests and understandings.

Research conducted in the ITAIDE project attempted to distinguish between different levels of stakeholders related to the data pipeline. (Stijn, et al., 2011) presented such a distinction between four levels of stakeholders: 1) national stakeholders within a region 2) national stakeholders in another region 3) stakeholders at the regional / economic zone and 4) international stakeholders. Table 1 provides an overview of these stakeholders and their activities, along with their primary role in the data pipeline (benefiting from or enabling the use of the pipeline).

LEVEL	EXAMPLES	ROLE	DETAILS
NATIONAL STAKEHOLDERS (levels 1&2)	Agencies	Benefit / Enable	Customs and Ministries (eg. Agriculture, ICT and Economics)
	Trading businesses	Benefit	Both multi-nationals and small companies
	Sea carriers	Benefit	
	Container Terminals	Benefit	
	Logistic service providers	Benefit	
	Port authorities	Benefit	
	Providers of Port Community Systems (PCS)	Enable	A PCS enables all the links within a logistics chain for the exchange of data
	Providers of the e-Government infrastructure	Enable	A national message broker, or a single window IT infrastructure to public service providers
	Consultants and Academics	Enable	
STAKEHOLDERS AT THE REGIONAL / ECONOMIC ZONE (level 3)	Freight Forwarders associations	Benefit	Most often they take responsibility for planning, arranging and optimizing shipments
	Large consignor or consignee councils	Benefit	Large consignors manage most of their supply chains by themselves and may use the pipeline to interact with other partners in the chain
INTERNATIONAL STAKEHOLDERS (level 4)	International Standardization Bodies	Enable	Standardization and interoperability efforts by bodies including WCO, ISO, UN/CEFACT, GS1)

Table 2A.1: Key stakeholders linked in the data pipeline. Sources: (Stijn, et al., 2011) (Overbeek, et al., 2011)

In practice, stakeholders are cooperating in sub-groups, throughout the different phases of the movement of goods, such as export, transfer and import. Such sub-groups of stakeholders within the supply chain form the so-called communities and it is usually the case that an actor is simultaneously a member of more than one community (Pruksasri, et al., 2012). Figure 2A.4 shows an example of such stakeholder communities.

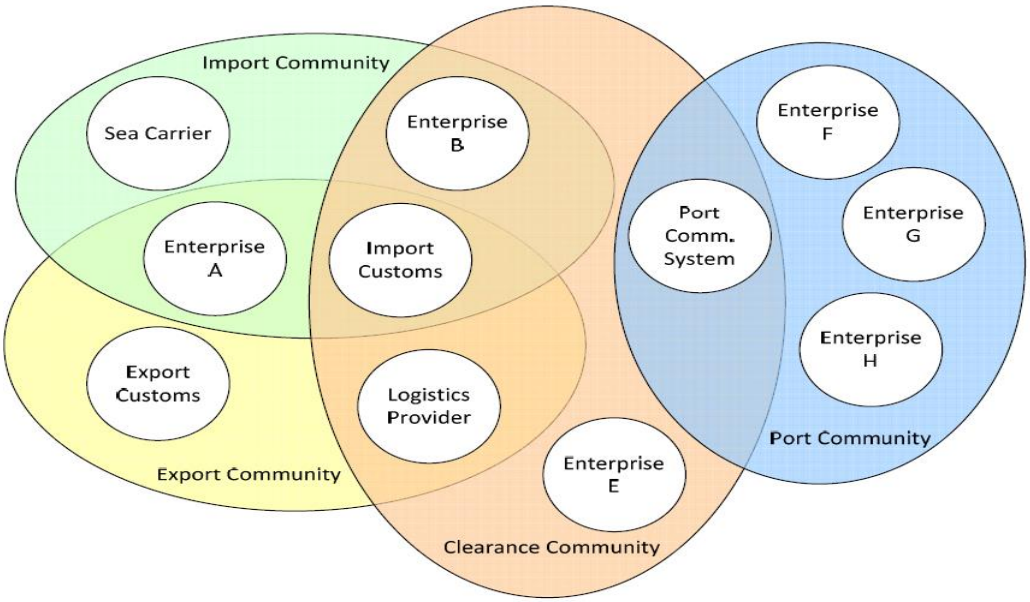

Figure 2A.4: Supply chain stakeholder communities. Source: (Pruksasri, et al., 2012)

Appendix 2B: Details on the pipeline configuration for the described case

In order to integrate information and enhance visibility across the supply chain, development is split between Seacon and GS1. GS1's ezTrack System can effectively track and trace the flow of goods and product information throughout the supply chain, by the means of an Electronic Product Code platform (EPCIS), which is also directly connected to the Malaysian Custom Authorities at the moment (GS1, 2012). Nevertheless, in order to integrate additional consignment and organization information, a connection between the Seacon and GS1 systems will be required in order to provide the intended pipeline solution. These systems will be used as a means for data capturing and storing, and also to provide a Supply Chain view (through a visibility dashboard) both to business parties in Malaysia and the Netherlands and to Customs (CASSANDRA, 29-04-2012).

It is evident that at the moment, there is no system connecting the export and import sides and the configuration of the data pipeline aims towards this direction. In order to reach this goal, however, actions such as creating an accessible data store, capturing event messages and creating visibility dashboards have been identified as necessary steps for the configuration of the pipeline. Different configurations are possible, for instance regarding which dashboard will provide a view for which actors. An example of such a configuration is presented in figure 2B.1.

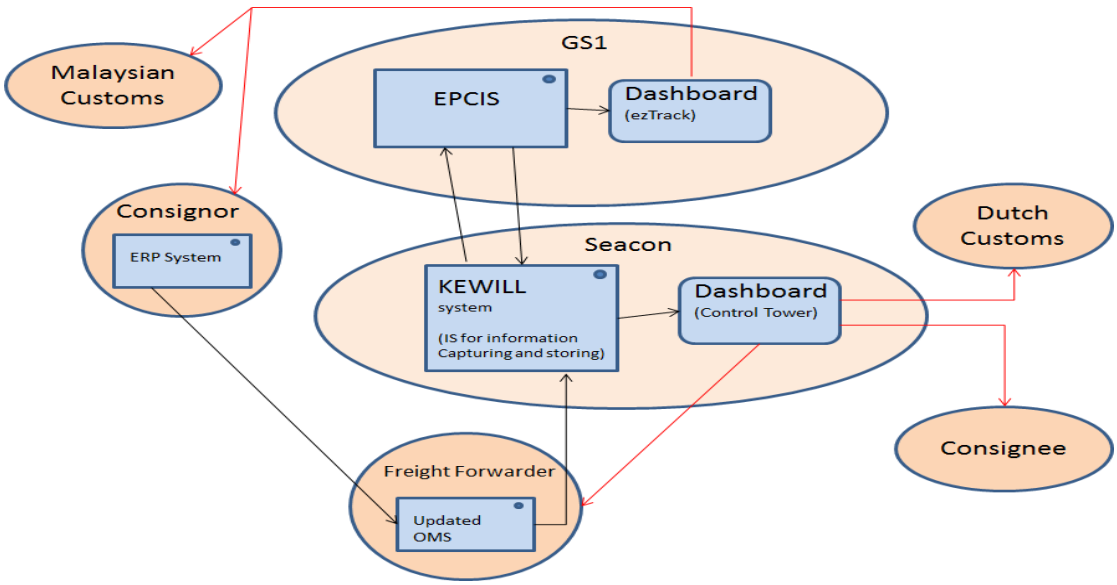

Figure 2B.1: Information exchange for enhanced visibility. Adapted from (CASSANDRA, 29-04-2012)

In this figure, the grey arrows indicate the upload of information from a certain source and the red arrows the possibility of accessing information via the dashboards when requested. Note that there are different possible configurations; for instance the Freight Forwarder could get a view of the information through the GS1 dashboard, or upload their data to the EPCIS system instead. In any case, the Seacon and GS1 systems are linked and, in essence, whatever solution is adopted in the end -depending on practical considerations- makes little difference for the purposes of this thesis.

Appendix 3A: Detailed description of the TSB services and functions

This section provides a detailed overview at the services the TSB is able to offer, as well as the functions which are necessary in order to provide these services, keeping in mind that the TSB is an architecture based on the principles of Public Key cryptography. At this point we must also note that the services and functions we are about to describe are related to the **TSB *architecture* as a whole.** In this sense, some services and functions are *supported by the TSB system/hubs* (for instance the core services and functions) and involve actions performed both by the TSB system and the end-entities, while others (for instance most enabling services and functions) are mainly performed by the TSB system itself. We have discussed that the primary role of the TSB architecture is to provide trust; in essence this means that the TSB is able to offer services in order to guarantee that the core security requirements with regard to the messages exchanged between actors are fulfilled. This can be considered as a means to an end, which is secure information exchange in various contexts (eg. secure e-mail, Electronic Data Interchange (EDI), web accessing etc.).

3A.1 Core services and functions

Before we start we must make clear that notions such as integrity and confidentiality will refer to the messages that are being exchanged. The integrity and confidentiality of the internal TSB components (for instance keys and certificates) is related to the security concerns for the TSB system itself and are examined in chapter 4.

1) Authentication. Perhaps the most obvious purpose of the TSB architecture is to offer the service of authentication. In comparison with technologies such as Kerberos and Microsoft.NET Passport, where authentication is primarily based on user-selected passwords, the TSB authentication service is rather based on public key cryptography, as in PKIs (Lopez, et al., 2005). This service can refer to:

- Data origin authentication
- Entity authentication

In both cases, the main related function is employing a *digital signature*. (Adams & Lloyd, 2002). The signature may be computed over the *hash* – a one-way mathematical function – of one of the following three values:

a) A message to be authenticated
b) A request that a particular actor intends to send to a remote device
c) A random challenge

The first is related to the service of data origin authentication and the latter two support the service of entity authentication (Adams & Lloyd, 2002).

2) Message Integrity. Another core service of the TSB is ensuring non-alteration of the transmitted messages, meaning that the data has not been undetectably altered. For obvious reasons, guaranteeing message integrity is essential in the international supply chain environment. The service of message integrity can again be achieved by the function of calculating a digital signature. Apart from enabling the service of authenticity, digital

signatures simultaneously provide integrity over the signed data. Any change in the input data will lead to an unpredictable change in the hash output and therefore the signature will fail to verify (Adams & Lloyd, 2002). An alternative function employed for integrity, as well as authentication, involves a *Message Authentication Code* (MAC).

3) Confidentiality. The service of protecting the confidentiality of the transmitted messages relates to keeping the information secret, so that only the intended recipient will be able to understand the message (Choudhury, et al., 2002). Again, this service requires the functions of both symmetric and public key cryptographic techniques. A description of how these mechanisms are employed in order to provide the main three services was presented in section 3.5, after further details about the logical components of the TSB architecture are provided.

The aforementioned services comprise the core services provided by the TSB architecture. In conjunction with traditional networking and communication protocols, these services will be used to provide secure communication in various contexts, such as secure e-mail (using for example a S/MIMEv3 protocol) and secure web server access (using a protocol like SSL or TLS). To be more specific, secure e-mail can be achieved by having the mail package access these core TSB services in order to encrypt and sign messages and format the result using the S/MIME syntax (Adams & Lloyd, 2002). By this, messages can be transported across an untrusted network without the risk of compromising their authenticity, integrity and confidentiality. An example in the context of the described logistics case was presented in section 3.5.

3A.2 Additional services and functions

Nevertheless, the notion that the TSB can provide trust to the actors involved in the described supply chain scenario, involves more than guaranteeing the authenticity, integrity and confidentiality of the messages. In this sense, additional TSB services and functions are:

4) Non-repudiation. Considering the business context surrounding the TSB architecture, it is apparent that non-repudiation services are very important for the TSB relying parties. Non repudiation refers to the service that ensures, at least up to a certain extent, that entities remain honest about their actions. The most common variants of this service are non-repudiation of origin (a user cannot falsely deny having originated a message) and non-repudiation of receipt (not denying receiving a message). The basic concept is that "*a user is cryptographically bound to a specific action in a way that subsequent denial of that action constitutes an admission of malice or negligence*" (Adams & Lloyd, 2002). Since a message, or a receipt, is signed by a private key which is only known to the signor alone, he can no longer dispute the fact of signing that message. At this point, we should note that non-repudiation is not a stand-alone service, since it usually relies on other services and functions. In particular, the time-stamping service is required to provide evidence that an event occurred at a specific time and the notarization service can facilitate storing this evidence. These services will be further discussed below. Finally, it should be also made clear that the TSB supports non-repudiation rather than provides it, since actors are also directly involved in a potential dispute resolution. In this sense, the TSB functions to create, maintain and archive some of the evidence that can be used in such a resolution.

5) Access control. Although the primary aim of digital certificates is to provide an authentication infrastructure, we still propose that the TSB should enable requesting entities to delegate access rights to other entities at will. In this sense, the TSB should ensure the granting of rights, including the ability to access specific information. For instance, some of the most sensitive information in Seacon's databases should only be accessible to specific actors, for instance the Malaysian Freight Forwarder or customs. Digital certificates can be also used as a basis for authorization, by the mapping of actors. In addition to key-binding certificates, *attribute certificates* can be used to bind some attribute values with identification information about their holder. According to (rfc5755, 2010), the attribute certificate is logically bound to the public key certificate, although it is a separate data structure. In this sense, the TSB can also function as an *Attribute Authority*, by assigning privileges to the different users via the corresponding attribute certificates, if necessary. Supporting functions include authentication, group definition, group update, rights update and user enrolment into a group.

6) Notarization. By the term notarization, we refer to the TSB service of certifying that a digital signature is valid. In this sense this service is related to asserting the correctness of data in a message through the following functions (Adams & Lloyd, 2002):

- Certifying that the signature verification computation with the corresponding public key is mathematically correct.
- Certifying that the public key is still validly associated with the entity claiming to have signed the hash value.

The TSB does so through the mechanism of a digital signature. Hence, the entities need to possess a valid copy of the TSB's verification public key in order to trust the notarization itself. The notarization service also relies on time-stamping, since the time when the notarization was done must be included.

7) Time-stamping. In order to establish the existence of data at a certain moment in time, the TSB should offer Time Stamping services; in other words it also functions as a time-stamping authority. Time-stamps (TSs) are used to provide a proof that the signed data existed at a particular point of time. By indicating whether or not a digital signature was generated before the particular private key was expired or compromised, the time-stamp service can greatly facilitate the services of non-repudiation and authenticity. Various time-stamping protocols are presented in the literature. We propose the adoption of the Improved Arbitrated protocol (Schneier, 1996), since it is a simple and effective protocol when an honest Trusted Third Party to run the time-stamping service exists. In our case it is the TSB with the task to undertake this responsibility. Figure 3A.1 describes the functions involved in the time-stamping process.

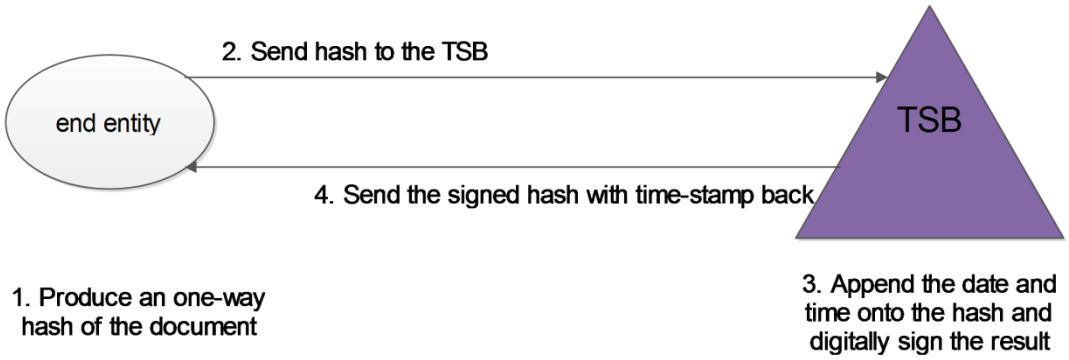

Figure 3A.1: Time-stamping protocol

The TSB can be considered a trusted party for running the time-stamping service by all supply chain actors, particularly if it was initiated as a joint venture (as discussed in section 2.2). However, and considering that such a business environment may require additional reliability even for time-stamping services, a more advanced protocol can be considered, for instance linking an actor's request for a time-stamp to previous requests. Since the order the TSB receives the different requests cannot be known in advance, if a time-stamp is challenged the originators of the previous and following time-stamped documents can be contacted. This protocol dismisses the possibility that the TSB can collude with an actor in order to produce a time stamp with a different time than the actual one and is known as the linking protocol (Schneier, 1996).

8) Privacy in communications. Although public key encryption can enable the confidentiality of the messages, the observation of the communication relations themselves may give away some information about the contents (Daskapan, 2012). In order to provide privacy, an option is to issue anonymous certificates. In this case, the TSB knows the true identity of an actor, but issues certificates that hide this identity from the rest of the world (Adams & Lloyd, 2002). However, since such an implementation of the service can prove to be complex and difficult to manage, an alternative solution for the supply chain actors is to camouflage communications by adding dummy messages into the data stream. By this, real data transfers can be hidden, both in terms of their frequency and occurrence. In any case, acknowledging that such functions may be quite ambitious to implement and also taking the TSB context into consideration, privacy in communications should be considered as an optional service of the TSB architecture.

3A.3 Enabling Services and Functions

9) Registration. Before supply chain actors can use the services of the TSB, they must first register. The primary goal of this service is to establish a unique binding between a user and his public key (Choudhury, et al., 2002). Typical functions involved in the process of registration include initial request submission, entity identification and authentication and registration information results. A more comprehensive overview of our proposed TSB initialization protocol in the particular business context was provided in section 3.5.

10) Key life-cycle management. It is evident that key management is a service of paramount importance within the TSB architecture. It relates to the life-cycle management of

cryptographic keys in a proper, efficient and secure way. Key management involves different functions which are now going to be described in more details:

- *Key pair generation:* This initial step consists of the generation of a private/public key pair through an appropriate cryptographic algorithm, as it is discussed in the next section. We propose that the TSB architecture must allow each entity to use whichever algorithms suit it for its own key pairs, according to the (rfc4210, 2005) management protocols. Although key pairs may also be generated in advance, we also propose that for additional reliability this process should be done in response to the registration process. In addition, it should be possible that each entity can possess more than one-key pair; for instance one key pair may be used to ensure confidentiality and another to support non-repudiation services: a commonly practiced two-key pair model. Finally, it should be noted that keys can be generated either within the end-entity's client system or within the TSB; nevertheless, when a pair is used for non-repudiation purposes, it should always be generated within the client system, so that the private key is never revealed to anyone else, including the TSB itself (Adams & Lloyd, 2002).
- *Key distribution:* The function of key distribution depends on the location where the key pair was generated. If it was generated by the client, then the public key must be securely conveyed to the TSB in order to be placed with a certificate. In case the key material was generated within the TSB, then it is the private key which must be distributed to the owner of that key. Mechanisms for secure key distribution, such as the ones described in (rfc4210, 2005), will be further discussed in chapter 4.
- *Key backup and recovery:* An optional function (determined by the TSB security policy) is that the TSB can hold a backup of the actors' keys in order to be recovered in case they are lost, so that permanent loss of enterprise information is avoided. In any case, it should be possible for actors to indicate whether backup is desired during the registration/initialization process. However, we must note that also for this function, private keys designated to support non-repudiation should never be backed up by the TSB (Choudhury, et al., 2002).
- *Key update:* Certificates issued by the TSB (and consequently bound key-pairs) are assigned a fixed lifetime upon issuance. In this sense, it is necessary to issue a new key pair (and the associated certificate) before expiration. (Adams & Lloyd, 2002) suggest that key updates should occur automatically once 70%-80% of the key lifetime has been exhausted.
- *Key history:* Since keys eventually expire and are therefore constantly updated, the TSB should be able to reliably store keying material necessary for decryption purposes when the corresponding certificate has expired. By this function, data that were encrypted with an expired key will be recoverable.
- *Key archival:* This function differs from key history in the sense that it is performed by the TSB for audit purposes and also to resolve disputes, particularly in combination with time-stamping and notarization services (Adams & Lloyd, 2002).

11) Certificate life-cycle Management. This service involves functions which are required to manage every facet of the digital certificate life cycle. These functions are:

- *Certificate creation:* Once a key pair has been generated, a digital certificate must be created in order to ensure the binding between the entity and its public key. Regardless of where key generation occurred, the function of creating the corresponding binding certificate is a responsibility of the TSB.
- *Certificate distribution and dissemination:* Once the certificate has been created, it must be distributed appropriately, depending on the intended key usage. For instance, a given certificate might be distributed directly to the owner (for instance via an in-band protocol distribution), or to a TSB database, which functions as a repository. By posting certificates in the TSB repository and offering the corresponding **directory services**, the TSB will enable entities to access on-demand a particular certificate when required, thus facilitating certificate retrieval. Protocols for the secure distribution and dissemination of certificates include the X.509 CMP specified in (rfc4210, 2005).
- *Certificate retrieval.* The need to retrieve a particular certificate is associated with two distinct usage requirements: Encrypting data destined for another entity (the sender must possess the receiver's public key in order to encrypt the symmetric key, as discussed previously) or verifying a digital signature received from another entity. (Adams & Lloyd, 2002). Certificates need to also be validated by end-entities in order to ensure that their integrity is sound and that it has not been expired or revoked. The TSB is involved in such a process of certificate validation, during the initialization phase which was described in section 3.4.
- *Certificate renewal and update.* When a certificate expires, the TSB can perform one of the two following functions. Either renew the certificate by placing the same public key into a new certificate, or update the certificate, by issuing a new certificate for a newly generated key (Choudhury, et al., 2002).
- *Certificate Revocation.* This function is related to the cancellation of a given certificate, before it actually expires.

It is evident that key and certificate life-cycle management functions are crucial for the smooth and efficient delivery of the most important TSB services. Some of these functions are by the TSB system itself without involving end-entities (eg. key backup) and others facilitate actions performed by users (eg. certificate retrieval), but they are all essential in order to guarantee that all actors can securely exchange information with each other. Figure 3A.2 gives an overview of these functions.

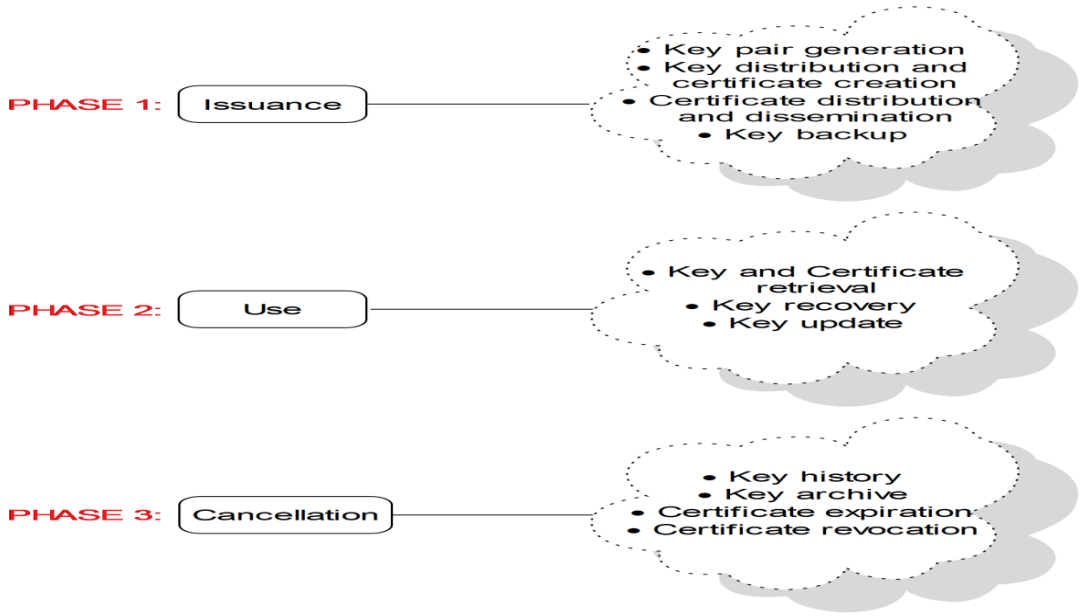

Figure 3A.2: Key and certificate life-cycle management functions

12) Data archival. This service maintains the collection of critical data for the operation of the TSB system. Several types of operational data, including details about subscribed entities and data for system recovery purposes should be archived and maintained in order to ensure the smooth delivery of the TSB services.

Appendix 3B: Alternative description of the TSB initialization protocol

The following figure provides a different illustration of the TSB initialization protocol for a Seacon and a FF entity, assuming that *both* entities are already a part of the local PKIs. In addition, in this figure, the local chains of trust are also depicted.

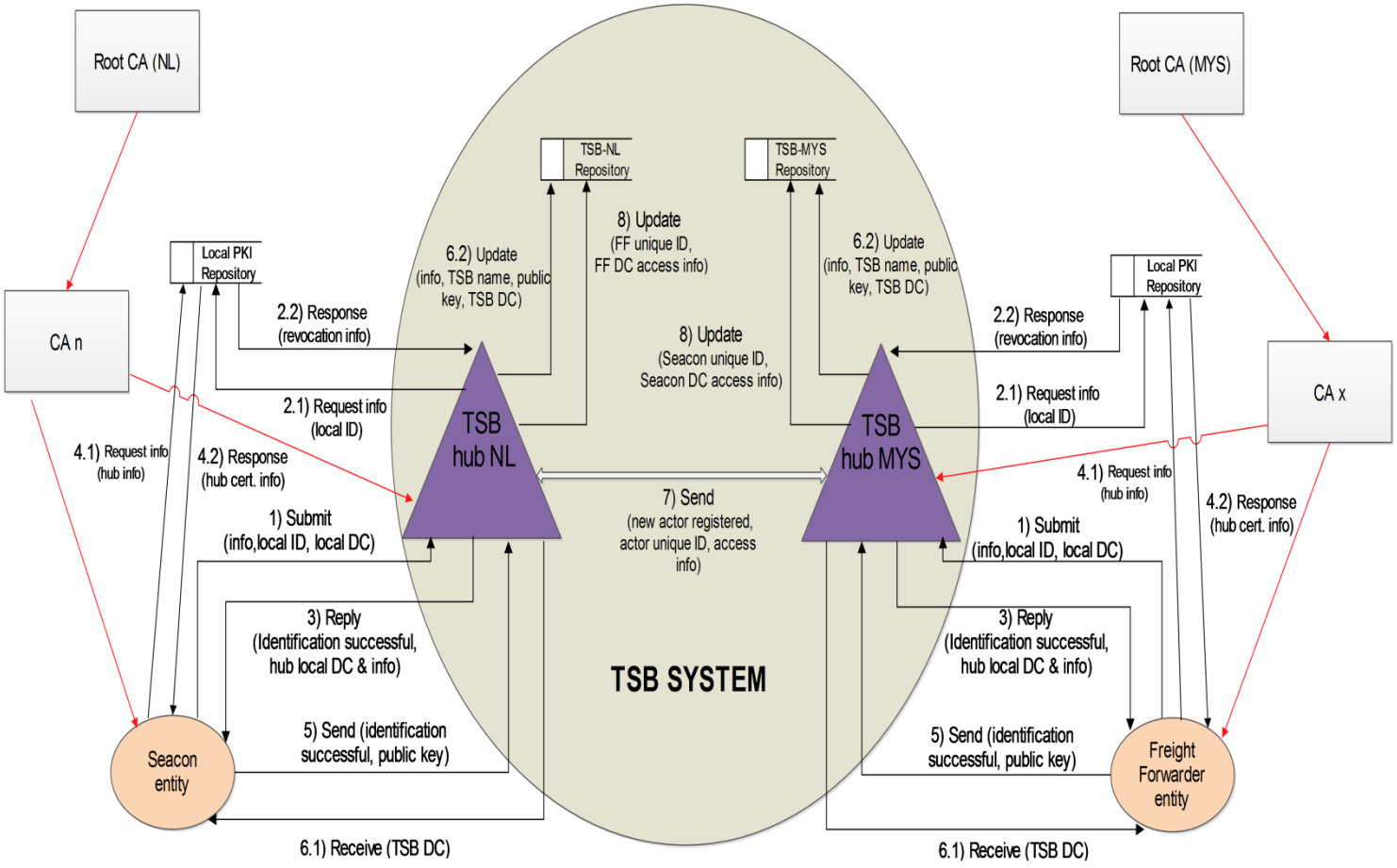

Figure 3B.1: TSB initialization protocol including chains of trust

Appendix 3C: Alternative visualization of the e-mail scenario

Note that the focus here is on the encryption/decryption processes. For this reason we simplified the process of certificate retrieval (requiring the involvement of both hubs). For a detailed description of this process the reader should refer to figure 3.7.

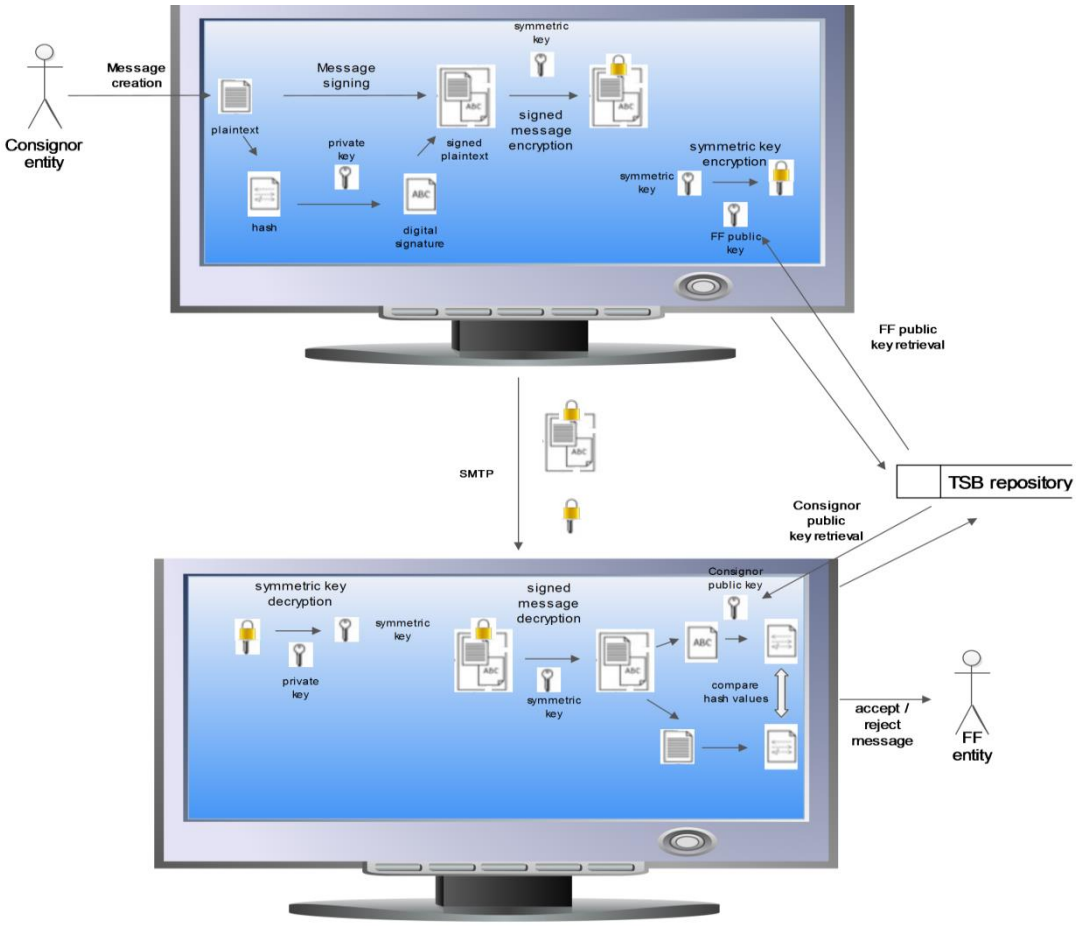

Figure 3C.1: Exchange via e-mail

Appendix 3D: Web-based communication scenario

Apart from e-mail communication, supply chain partners may interact through web-based applications, as it happens for example between Seacon and the Malaysian Freight Forwarder. At this point it should be made clear that the notion of "Linked Data", which finds application in the data pipeline, essentially implies that information can be retrieved automatically, without client (human) entity involvement (i.e. server to server). However, for simplicity purposes we will assume that the data contained in the FF's databases – and are available through a web server – are requested by a Seacon client, which makes little difference for the purposes of this Thesis. In the following example, we will present the process of establishing a secure communication path between the Seacon client and the FF web server, through the SSL protocol. Since the FF database contains sensitive information, client authentication should be considered mandatory. For this reason, we assume that SSL v3 is used, since it allows for client authentication (IBM, 2013). The following sequence diagram describes the "handshake" process (Tanenbaum & Wetherall, 2011) between these two entities.

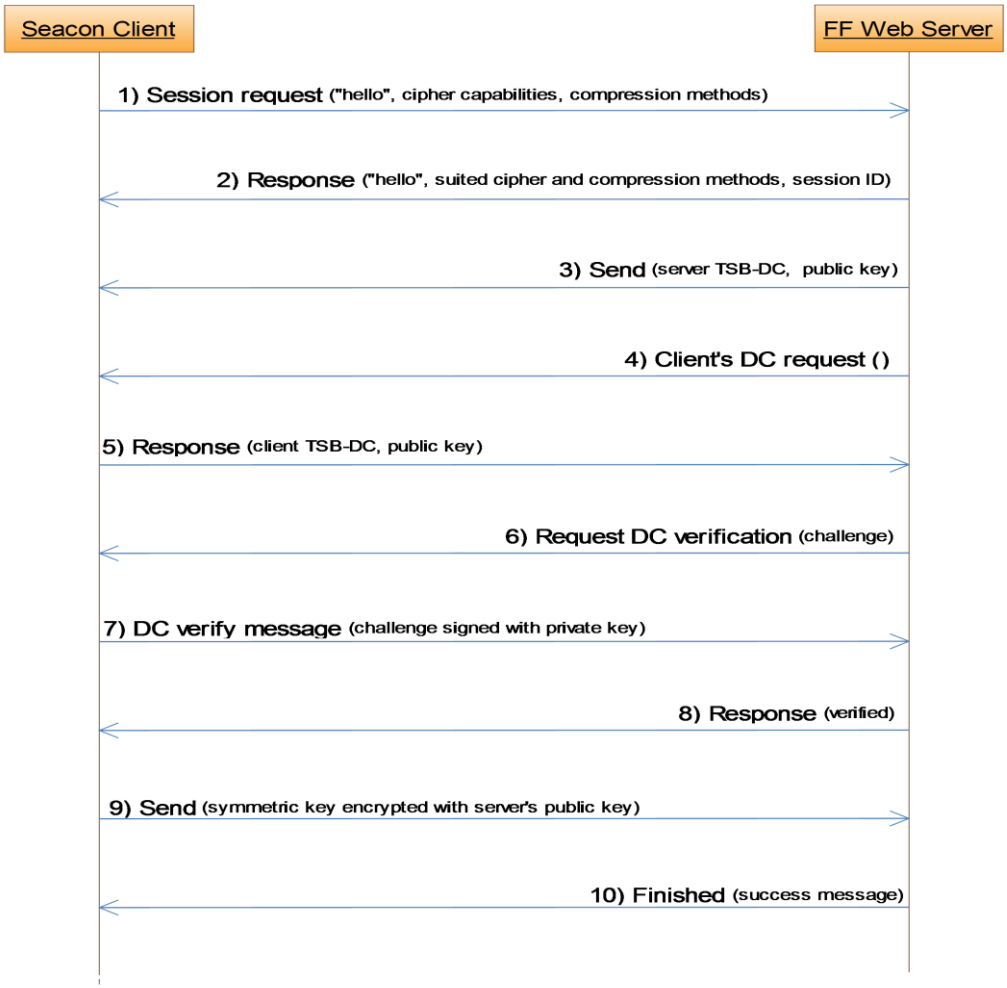

Figure 3D.1: SSL handshake between a Seacon client and the FF web server.

It should be clear that, in this case, the TSB digital certificates that the two entities possess are useful for authentication purposes. While it is essential that the client should directly authenticate himself, the same does not apply for the web server. If the server is not the legitimate owner of the certificate, then it will be impossible to decipher the symmetric key and therefore communication will not be achieved. We must also note that this is a rather simplified overview; for instance the process of generating a symmetric key involves a pre-master secret which is subsequently converted into the master secret (IBM, 2013). In addition, to deal with authorization issues, it may be mandatory that the server also asks for an attribute certificate. Finally, although the certificates could also be retrieved from the TSB repositories, we rather adopted this approach in order to stick with the SSL conventions.

Regarding to the TSB role in this process, we can argue that it is rather implicit: by providing the certificates to both entities, a successful SSL handshake is possible. In addition, since the two entities have been certified by different TSB hubs, they may request from their local hubs to validate the certificates when they receive them. In any case, the role of the TSB should not be underestimated: apart from the initialization process, the TSB also performs supporting functions independent from the actors (most notably key and certificate life-cycle management), so that the exchange of information, as in the cases previously described, can be performed securely and efficiently.

Appendix 4A: Detailed methodology description

Our primary focus will be to protect the *assets* within the *online distributed* systems that form the core of the TSB architecture from malicious intrusions. According to the National Institute of Standards and Technology (NIST) a *risk* is dependent on the probability of a given *threat* exploiting a potential *vulnerability* and the resulting impact on the system or organization (Daskapan, 2012). The assets under consideration can be any data or component of the TSB architecture (as defined in chapter 3) that supports information-related activities. Anything that is capable of acting against such assets in a manner that can result in a harm or loss is considered a threat. Vulnerability is a weakness in the system that may be exploited. It is apparent that a risk assessment is necessary in order to identify such threats and vulnerabilities and quantify their potential impact. Based on the results of such an assessment, we can then proceed on determining the proper security controls that need to be in place in order to minimize the risks and their impact.

The first step is to identify the most relevant assets with regard to the TSB and classify them across three distinct qualitative asset classes: High Business Impact, Medium Business Impact and Low Business Impact. A compromise of a HBI asset causes a severe or a catastrophic loss to the organization. Examples of such assets include credentials, highly sensitive business material and personally identifiable information (PII). A compromise of a MDI asset can cause a moderate loss to the organization. An example of this class is internal business information. Finally, LBI assets are typically not confidential and an unauthorized disclosure would typically not result in significant financial loss, operational disruptions or competitive business disadvantage (Microsoft, 2006).

The second step is to identify potential threats and vulnerabilities. In order to do so, it is beneficial to first determine applicable Defense-in-Depth layers for each asset in order to provide structure and pertain to all elements of risk. These layers are physical, network, host, application and data. For each applicable layer, potential threats and vulnerabilities are identified. To put it simply, it is determined what we are trying to avoid (threat) and how it may actually happen (vulnerability).

The third step involves estimating the asset exposure and the overall business impact. Asset exposure refers to the extent of the potential damage to an asset (H,M,L), regardless of the asset class definition. The overall impact is then based on both asset classification and exposure, as described in figure 4A.1.

Impact Rating Reference

Asset Class	**High**	Moderate	High	High
	Med	Low	Moderate	High
	Low	Low	Low	Moderate
		Low	**Medium**	**High**
		Exposure Level		

Figure 4A.1 Estimating overall impact rating. Source (Microsoft, 2006)

The fourth step involves defining the current controls for each layer related to the asset and determining the probability (H,M,L) of the impact occurring. This probability consists of two elements. The first depends on attributes of the probability and possible exploit. Some common attributes include: attacker population, local vs. remote access, visibility of exploit and automation of exploit. A guideline on assigning probabilities based on these attributes is given in figure 4A.2. The second is related to the effectiveness of current controls. Finally, given the likelihood (based on exploit attributes) and the effectiveness of the corresponding current controls, an overall probability of the impact is assigned.

Probability Definitions for Vulnerabilities
High
Large attacker population- "script-kiddie"/hobbyist
Remotely executable
Anonymous privileges needed
Externally-published exploitation method
Automated
"5" if any apply
Medium
Medium attacker population - expert/specialist
Non-remotely executable
User level privileges required
Not publicly-published exploitation method
Non-automated
"3" if any apply
Low
Small attacker population - insider knowledge
Non-remotely executable
Administrator level privileges required
Not publicly-published exploitation method
Non-automated
"1" if all apply

Figure 4A.2: Probability definitions. Source: (Microsoft, 2006)

The final step involves estimating the overall risk rating for each layer, based on both the impact rating and the impact probability. Figure 4A.3 describes the process of estimating the overall risk level based on these two values.

		Risk Rating		
Impact (from Impact Table above)	**High**	Moderate	High	High
	Med	Low	Moderate	High
	Low	Low	Low	Moderate
		Low	**Medium**	**High**
		Probability Value		

Figure 4A.3: Overall risk rating. Source: (Microsoft, 2006)

Based on the risk assessment results, we can prioritize and define the corresponding security controls, which address the security requirements of availability, integrity, confidentiality, authentication, access control and non-repudiation for each asset class. In order to select the proper security controls, we will rely on both the risk assessment results and the recommendations stemming from the MSAT tool, which is based on best industry practices for organizations similar to the TSB hubs.

Appendix 4B: Asset clusters

(In bold are the assets selected for the risk assessment from each cluster)

Asset class	Asset Name	Asset Rating
High level description of asset	*Definition*	*Asset Rating (high, medium, low)*
Physical infrastructure	**Data centers / servers**	**HIGH**
Physical infrastructure	Network switches	HIGH
Physical infrastructure	Routers	HIGH
Physical infrastructure (software)	**End-user TSB application**	**HIGH**
Physical infrastructure	**Desktop computers**	**LOW**
Physical infrastructure	PDAs	LOW
Physical infrastructure	Cell phones	LOW
Physical infrastructure	Removable media (tapes, floppy disks, CD-ROMs, DVDs, portable hard drives, PC card storage devices, USB storage devices,etc.)	LOW
Physical infrastructure	Fax machines	LOW
Physical infrastructure (software)	Development tools	LOW
Physical infrastructure (software)	Server/desktop software	LOW
Intranet data	**TSB-hub private key**	**HIGH**
Intranet data	Financial data	HIGH
Intranet data	Employee passwords / private keys / biometric identifiers	HIGH
Intranet data	Intellectual property	HIGH
Intranet data	Strategic plans	HIGH
Intranet data	**Operational data**	**MEDIUM**
Intranet data	Employee personal contact data	MEDIUM

Intranet data	Network infrastructure design	MEDIUM
Intranet data	Internal Web sites	MEDIUM
Extranet / internet data	**Supply chain actors' cryptographic keys and TSB identity**	**HIGH**
Extranet / internet data	Actor personal and financial data	HIGH
Extranet / internet data	Actor contact data	MEDIUM
Extranet / internet data	**TSB public key**	**MEDIUM**
Extranet / internet data	Web site marketing data	MEDIUM

Table 4B.1: Asset clusters

Appendix 4C: List of common threats

Threat	Example
High level description of the threat	*Specific example*
Catastrophic incident	Fire
Catastrophic incident	Flood
Catastrophic incident	Earthquake
Catastrophic incident	Severe storm
Catastrophic incident	Terrorist attack
Catastrophic incident	Industrial accident
Mechanical failure	Power outage
Mechanical failure	Hardware failure
Mechanical failure	Network outage
Mechanical failure	Environmental controls failure
Mechanical failure	Construction accident
Non-malicious person	Uninformed employee
Non-malicious person	Uninformed user
Malicious person	Hacker, cracker
Malicious person	Computer criminal
Malicious person	Industrial espionage
Malicious person	Government sponsored espionage
Malicious person	Social engineering
Malicious person	Disgruntled current employee
Malicious person	Disgruntled former employee
Malicious person	Terrorist
Malicious person	Negligent employee
Malicious person	Dishonest employee (bribed or victim of blackmail)
Malicious person	Malicious mobile code

Table 4C.1: Common Threats. Adapted from (Microsoft, 2006)

Appendix 4D: List of common vulnerabilities

Vulnerability Class	Vulnerability	Example
High level vulnerability class	*Brief description of the vulnerability*	*Specific example (if applicable)*
Physical	Unlocked doors	
Physical	Unguarded access to computing facilities	
Physical	Insufficient fire suppression systems	
Physical	Poorly designed buildings	
Physical	Unlocked windows	
Physical	Walls susceptible to physical assault	
Natural	Facility located on a fault line	
Hardware	Missing patches	
Hardware	Outdated firmware	
Hardware	Misconfigured systems	
Hardware	Systems not physically secured	
Hardware	Management protocols allowed over public interfaces	
Software	Out of date antivirus software	
Software	Missing patches	
Software	Poorly written applications	Cross site scripting
Software	Poorly written applications	SQL injection
Software	Poorly written applications	Code weaknesses such as buffer overflows
Software	Deliberately placed weaknesses	Vendor backdoors for management or system recovery
Software	Deliberately placed weaknesses	Spyware such as keyloggers
Software	Deliberately placed weaknesses	Trojan horses
Software	Configuration errors	Systems not audited
Software	Configuration errors	Systems not monitored
Communications	Unencrypted network protocols	
Communications	Connections to multiple networks	
Communications	No filtering between network segments	
Human	Poorly defined procedures	Insufficient incident response preparedness
Human	Poorly defined procedures	Insufficient disaster recovery plans
Human	Stolen credentials	

Table 4D.1: Common Vulnerabilities. Adapted from (Microsoft, 2006)

Appendix 4E: Sample of Input questionnaire for the MSAT tool

Assessment Question	Your Answer
Business Risk Profile	
Number of desktops and laptops in use at your company:	50 to 149
Number of servers in use at your company:	6 to 10
Does your company maintain a full-time connection to the Internet?	Yes
Do customers and vendors access your network or internal systems via the Internet?	Yes
Does your company host application services, such as a portal or a Web site, for external customers or partners?	Yes
Does your organization deploy services that are used by both external and internal clients in the same network segment?	Yes
Do external partners or customers connect directly to your company's internal, back-end systems for the purposes of data access, record updates, or other information manipulation?	Yes
Has your organization deployed the same back-end infrastructure components, such as databases, to support both external applications and internal corporate services?	Yes
Does your organization allow employees or contractors to connect remotely to the internal corporate network?	No
Does your organization allow employees to deploy non-production systems, such as personal Web servers or computers housing "pet projects," on the general corporate network?	No
Aside from backup tapes/media, does your organization allow confidential or proprietary data off-site for processing?	No
Would a compromised system's security significantly impact your company's ability to conduct business?	Yes
Does your company share office space with other organizations?	No
Does your company develop applications?	Yes
Does your organization allow software developers to connect remotely to corporate development resources or remotely develop application code?	No
Does your company develop and market software products for customers, partners, or a broad market?	Yes
Does your organization allow developers to run development or test systems in remote or unprotected locations?	No
Does your IT staff act as the custodian (as opposed to developer) of line of business applications?	No
Do your business processes require data that is stored, processed, or distributed by a third party?	No
Does your company store or process customer data in an environment that is shared with corporate resources?	No
Do you rely on third-party software development partners to support business-service offerings?	No
Does your company generate revenue based on service offerings that require data processing or data mining?	Yes

Does your organization consider the data processed by your company's application services sensitive or critical to your customers' business operations?	Yes
Does your company make its critical business applications available through Internet-based connections?	Yes
Who are the target users of the key applications within your environment?	Both internal employees and external customers, vendors, and partners
How is access to key applications made available to users?	Both from within the internal network and remotely
Does your corporate network connect to customer, partner, or third-party networks via network links, whether public or private?	Yes
Does your company generate revenue from services based on the storage or electronic distribution of data, such as media files or documentation?	Yes
Has your organization gone through a "rip and replace" change of any major technology component in the last 6 months?	No
Does your company rely on receiving data feeds or processed data from partners, vendors, or other third parties?	Yes
Would an incident that affected customer applications or infrastructure, such as a site outage or a hardware or application failure, impact revenue?	Yes
Does your company store sensitive or critical customer data?	Yes
Do customer infrastructure components or applications rely on access to resources within your environment?	Yes
Does your company share infrastructure and application components among multiple customers?	Yes
Do you consider information technology to be a requirement for your company?	Yes
Do all of the employees in your company use computers for business?	No
Does your company outsource maintenance or ownership of any portion of its infrastructure?	No
Does your company have a mid- or long-term plan for the selection and deployment of new technology components?	Yes
Do you consider your organization to be an early adopter of new technology?	Yes
Does your organization select and deploy new technologies based on existing partnerships and licensing agreements?	No
Does your organization limit technology choices to technologies known by the current IT staff?	No
Does your company expand its network through acquisition of new companies and their existing environments?	No
Does your organization allow employees to download sensitive customer or corporate data to their workstations?	No
Does your organization restrict access to information by users based on their role?	Yes
Does your organization deploy new services or applications before	No

assessing them for possible security issues?	
Does your organization change credentials for privileged accounts on a regular basis?	Yes
Does your organization change credentials for privileged accounts after termination of personnel with privileged access?	Yes
Choose the option that best describes your company's industry segment:	IT Services
Choose the size of your organization:	50 to 149 employees
Does your company have more than one location?	Yes
Is your company in a highly competitive or research-focused industry in which intellectual property theft or espionage is a significant concern?	Yes
Are the technologists in your company subject to high turnover or attrition?	No
Does your company have significant product or brand recognition?	No
Does your company use down version or legacy software (software that is no longer supported by the vendor)?	No
Does your organization acquire software from a reputable vendor or source?	Yes

*Note that this the tool has been used several times with slightly varying inputs in order to get a more spherical overview of the most relevant security controls that should be implemented and the above figure only describes one of these instances.

Appendix 4F: Complete risk assessment table

Asset					Exposure							
Risk ID	**Asset Name**	**Asset category**	**Asset Class**	**Applicable Defense-in-Depth Layer(s)**	**Threat Description**	**Vulnerability Description**	**Exposure Rating (H,M,L)**	**Impact Rating (H,M,L)**	**Current Controls Description**	**Probability (H,M,L)**	**Summary Risk Level (H,M,L)**	**Proposed controls**
1.2.1	TSB private key	Intranet data	HBI	Network	Unauthorized access to the hub's intranet	Connection of unauthorized local client to hub's intranet due to outdated configuration of perimeter defense mechanisms	L	**M**	1. Separation of critical internal hub resources from resources accessible to end entities. 2. No remote accessing of critical internal hub resources. 3. Intranet firewalls and intrusion detection systems in place. 4. No wireless connectivity to hub's intranet.	**M**	**M**	1. Deploy firewalls and other network-level access controls at each location and frequently test and verify that they are working properly. 2. Ensure that network-based intrusion detection systems' signatures are kept up-to-date.
1.3.1	TSB private key	Intranet data	HBI	Host	Unauthorized access to critical intranet data such as the TSB's private key through theft of credentials	Theft of credentials off managed LAN client via outdated configuration of antivirus signatures, host configuration, or outdated security patches	M	**H**	1. Restrict access to this data only to the TSB-hub senior managers. 2. Antivirus update and patches enforced on LAN every few hours - narrowing compromise of host during time window of exploit vs. patch. 3. E-mail notices to patch/update.	**H**	**H**	1. Multi-factor authentication mechanisms for highly-authorized individual's accounts. 2. Adding anti-virus client in the default workstation build environment. 3. Keep different types of data in separate places depending on their criticality.
1.4.1	TSB private key	Intranet data	HBI	Application	Unauthorized access to critical intranet data such as the TSB's private key by employees through improper exploitation of the TSB hub application (which accesses the TSB private key for the process of actor certification)	Exploitation due to code weakness	M	**H**	1. TSB application developed in-house. 2. Regular provision of patches and updates. 3. Authorization mechanisms that provide access to sensitive data and functionality only to suitably permitted application users.	**M**	**H**	1. Regular auditing of application configuration. 2. Quick response to identification of critical code weaknesses. 3. When a patch is made available, testing in lab-conditions is essential. 4. Collaboration with experienced third-party application developers to review the application. 5. Encrypt all sensitive data prior to transmission to other components.

1.4.2	TSB private key	Intranet data	HBI	Application	Unauthorized access to critical intranet data such as the TSB's private key through improper exploitation of the TSB hub application (which accesses the TSB private key for the process of actor certification)	Exploitation due to deliberately placed weaknesses, such as trojan horses and spyware	H	**H**	1. TSB application developed in-house. 2. Development team employee background checks. 3. Authorization mechanisms that provide access to sensitive data and functionality only to suitably permitted application users.	**L**	**M**	1. Regular auditing of application configuration. 2. Maintaining application logs to monitor when certain actions have been performed and by whom. 3. Encrypt all sensitive data prior to transmission to other components.
1.5.1	TSB private key	Intranet data	HBI	Data	Unauthorized access to critical intranet data such as the TSB's private key through theft of credentials	Theft of credentials **via** non-technical means (eg. eavesdropping) by trusted employees.	H	**H**	1. Restrict access to this data only to the TSB-hub senior managers. 2. Background checks on employees.	**L**	**M**	1. Multi-factor authentication mechanisms for highly-authorized individual's accounts. 2. Promotion of employee awareness. 3. Encrypt all sensitive data stored, through the strongest encryption algorithms, such as 3DES or AES. Use a key length of 128 bits at minimum (1024 bits for AES).
1.5.2	TSB private key	Intranet data	HBI	Data	Unauthorized access to critical intranet data such as the TSB's private key through terminated employees	Terminated employee credentials and accounts still active.	M	**H**	1. Restrict access to this data only to the TSB-hub senior managers. 2. Regular monitoring and management of inactive accounts.	**L**	**M**	1. Institute a process to include an immediate notification procedure to all system administrators for terminated staff members to ensure their accounts are disabled immediately. 2. Encrypt all sensitive data stored, through the strongest encryption algorithms, such as 3DES or AES. Use a key length of 128 bits at minimum (1024 bits for AES). 3. Define a formal exit policy and procedure, both for friendly and hostile exits of employees.
1.5.3	TSB private key	Intranet data	HBI	Data	Manipulation or disclosure of critical intranet data such as the TSB's private key by highly authorized employees.	Highly authorized employees can access sensitive data.	H	**H**	1. Restrict access to this data only to the TSB-hub senior managers. 2. Background checks on employees.	**L**	**M**	1. Encrypt all sensitive data stored, through the strongest encryption algorithms, such as 3DES or AES. Use a key length of 128 bits at minimum (1024 bits for AES). 2. Maintain access logs to databases containing critical data for prevention of malicious attempts (to guarantee proper auditing and non-repudiation)

2.2.1	Actor keys, DCs and info	Extranet / Interent data	HBI	Network	Disclosure of actor information through unauthorized connection to the hub's network	Unauthorized connection of **local** client to hub's network due to outdated configuration of internal perimeter defense mechanisms	L	**M**	1. Internal firewalls and intrusion detection systems in place. 2. No wireless connectivity to hub's intranet.	**L**	**L**	1. Deploy firewalls and other network-level access controls at each location and frequently test and verify that they are working properly. 2. Ensure that network-based intrusion detection systems' signatures are kept up-to-date.
2.2.2	Actor keys, DCs and info	Extranet / Interent data	HBI	Network	Disclosure of actor information through unauthorized connection to the hub's network	Unauthorized connection of **remote** client to hub's network due to outdated configuration of internal perimeter defense mechanisms and absence of segment filtering.	M	**H**	1. Internal firewalls and intrusion detection systems in place. 2. VPN for remote-user-access connectivity based on Secure Sockets Layer (SSL) is currently being used to secure access. 3. Network controls are in place to restrict access to only what is required for each third-party connection.	**H**	**H**	1. Deploy site-to-site connectivity based on IPsec technology. Configure network access lists and user access lists for restricting access to necessary corporate resources. 2. Use segmentation to separate specific extranets from different user access and restrict access between network segments. 3. Deploy one or more DMZs (demilitarized zones) as part of a systematic and formal firewall development. 4. Place all Internet accessible servers there. Restrict connectivity to and from the DMZs.
2.3.1	Actor keys, DCs and info	Extranet / Interent data	HBI	Host	Unauthorized access to critical extranet data such as actor keys and information through theft of credentials	Theft of credentials off managed **local or remote** client via outdated configuration of antivirus signatures, host configuration, or outdated security patches	H	**H**	1. Antivirus update and patches enforced on LAN every few hours - narrowing compromise of host during time window of exploit vs. patch. 2. E-mail notices to patch/update. 3. Actor private keys are never conveyed to the TSB.	**H**	**H**	1. Two-factor authentication mechanisms for all users, local and remote, with smart card issuance apart from passwords. 2. Adding anti-virus client in the default workstation build environment. 3. Configuration of network access lists and user access lists for restricting access to necessary resources.

2.4.1	Actor keys, DCs and info	Extranet / Interent data	HBI	Application	Access to customer data by a party outside the TSB community via unauthorized use of the TSB end-entity application	Unauthorized use of the TSB application via poor authentication mechanisms.	H	**H**	1. TSB application is given to actors after they successfully complete the initialization protocol. 2. Application passwords are selected by actors.	**M**	**H**	1. Implement an authentication mechanism whose strength is commensurate with data criticality. Strong passwords should be 8 to 14 characters in length, with alphanumeric and special characters. 2. Minimum length, history maintenance, lifetime, and pre-expiration of passwords should all be set to provide additional defenses to password strength. 3. Account lockout, after 10 failed login attempts, should be enabled on all user accounts. 4. Applications should implement an authorization mechanism that provides access to sensitive data and functionality only to suitably permitted users or clients. 5. Role-based access controls should be enforced at the database level as well as at the application interface. 6. All attempts to obtain access without proper authorization should be logged.
2.5.1	Actor keys, DCs and info	Extranet / Interent data	HBI	Data	Disruption of actor-to-actor communication due to outdated information, loss of data or inability to retrieve partner info from the TSB databases	Data incorrect or lost due to mistakes or poorly defined procedures	H	**H**	1. Regular database (key, certificate and info) back-up. 2. Immediate update of actor information and revocation lists if a compromise is suspected by the actor.	**L**	**M**	1. Define roles and responsibilities among employees and promote security awareness in order to avoid costly mistakes.
3.1.1	Data centers / servers	Physical Infrastructure	HBI	Physical	Damage or theft of the equipment	Damage of critical infrastructure equipment via natural causes (eg. fire)	L	**M**	1. Alarm systems installed in equipment rooms.	**L**	**L**	1. Regular check of facilities
3.1.2	Data centers / servers	Physical Infrastructure	HBI	Physical	Damage or theft of the equipment by unauthorized access of third parties.	Unauthorized access to critical infrastructure equipment due to poor physical security procedures	H	**H**	1. Alarm systems installed in equipment rooms to detect break-ins 2. Data centers are in a locked room with restricted access.	**L**	**M**	1. Institute physical access controls against unauthorized personnel, such as employee and visitor badges. 2. Increase staff awareness of the personnel access control policy and encourage the challenging of unrecognized individuals.

3.3.2	Data centers / servers	Physical Infrastructure	HBI	Host	Setback of operations due to database/server being unavailable	Denial of service due to poorly defined procedures in case of high load or DDOS attacks.	H	**H**	1. Recovery and backup mechanisms	**H**	**H**	1. A more proactive approach is required. To ensure high availability for critical databases and servers, clustering mechanisms can be deployed. 2. Hardware load balancers can be deployed in front of web servers to achieve higher availability.
4.3.1	TSB operational data	Intranet data	MBI	Host	Unauthorized access to critical intranet data such as the TSB's private key through theft of credentials	Theft of credentials off managed LAN client via outdated configuration of antivirus signatures, host configuration, or outdated security patches	M	**M**	1. Each manager / account has access only to a part of the operational data, in order to reduce exposure levels. 2. Antivirus update and patches enforced on LAN every few hours - e-mail notices to patch/update.	**M**	**M**	1. Two-factor authentication mechanisms for authorized accounts (eg. smart card issuance in addition to passwords). 2. Keep different types of data in separate places depending on their type and criticality.
4.4.1	TSB operational data	Intranet data	MBI	Application	Disclosure or manipulation of operational data via the TSB-hub application.	Manipulation or loss of data due to missing patches	M	**M**	1. The development team identifies critical patches and applies them as soon as possible.	**M**	**M**	1.All applications should be periodically evaluated for security, backed up regularly, fully documented, and have contingencies in place in case they fail. 2. If there are any known application vulnerabilities that do not have available patches, determine when a patch will be available and develop an interim mitigation plan to address that vulnerability. 3. Avoid use of custom Macros.
4.5.1	TSB operational data	Intranet data	MBI	Data	Disclosure of operational data by authorized employees.	Disclosure of data via dishonest or disgruntled TSB employees.	M	**M**	1. Each authorized employee has access only to a part of the operational data, in order to reduce exposure levels. 2. Employee background checks.	**L**	**L**	1. Maintain access logs to databases containing critical data for prevention of malicious attempts (to guarantee proper auditing and non-repudiation) 2. Consider encrypting operational data with common algorithms such as DES,AES and blowfish.
5.5.1	TSB public key	Extranet / Interent data	MBI	Data	Disruption of actor-to-actor communication due to manipulation (or inability to retrieve) the TSB public key	TSB public key incorrect or lost due to mistakes and poorly defined procedures	H	**H**	1. Regular data back-up.	**M**	**H**	1. Define roles and responsibilities among employees and promote security awareness in order to avoid costly mistakes. 2. Immediate update of the database if a compromise of the TSB public key is suggested by the actors.

6.4.1	TSB application (as an asset itself)	Infrastructure	HBI	Application	Disruption of operations due to application malfunctions.	Malfunctions and glitches due to poor application development practices.	H	**H**	1. TSB application developed in-house. 2. Application development fully documented	**H**	**H**	1. Regular back-up of applications and maintenance of in-place contingencies 2. Regular provision of patches and updates
7.1.1	Workstations	Physical Infrastructure	LBI	Physical	Damage or theft of the equipment	Damage or theft of equipment via unauthorized access of third parties	L	**L**	No controls	**L**	**L**	1. In order to prevent theft, workstations can be secured with cable locks
7.3.1	Workstations	Physical Infrastructure	LBI	Host	Unauthorized access to personal employee workstations and data	Workstations can be left unattended by careless employees	L	**L**	No controls	**M**	**L**	1. All users should have a password-protected screen saver with a short time-out period.

Table 4F.1: Complete security risk assessment


TRUST