Trust broker Services

The Bachelor Series

Jericho in depth…

Trust broker Services

Defining trust in Jericho networks

Adriaan Bruning

Capgemini's Security & Innovation Research Centre, based in the Netherlands, focuses on near future IT Security solutions. The Jericho forum's vision on network de-perimeterization and Boundaryless Information flow™ has been the starting point for this research centre. Research papers from this centre appear in two distinct categories;

1. The Master Series

Researcher holding a masters degree in Informatics or are in the process of obtaining a master degree publish in the Master Series. The participating University and the Capgemini Security & Innovation Research centre have approved publications in this category.

Publications in this Series for 2008;

- Jericho in depth… Secure Communications by A. Stan
- Jericho in depth… The road to Jericho by A. Stan

Planned publications in this Series for 2008;

- Demystifying trust by F. van Leijden
- Jericho in depth… Automated Security Classification by K. Clark
- Jericho in depth… Trust Management for Trust brokers by A. Demarteau

2. The Bachelor Series

Researchers holding a bachelors degree in Informatics or in the process of obtaining a bachelors degree publish in the bachelor series. Their University and the Capgemini Security & Innovation Research centre have approved publications in this category.

Publication in this series for 2008;

- Jericho in depth… Endpoint security by L. Teheux
- Jericho in depth… Authentication and Accounting by E. Barannikov
- Jericho in depth… Trust broker Services by A. Bruning
- Jericho in depth… Trust broker framework by A. Bruning

Planned publications in this series for 2008;

- Jericho in depth… Controlling the COA framework by J. Willemsen
- Jericho in depth… Fully ASP based by D. Hanenberg & F. Aardoom

Copyright © Capgemini 2008

All rights reserved. No part of this work may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage and retrieval system, without the prior written permission of Capgemini.

Preface

Since the dawn of the Internet at the ending of 1969 a lot has changed, I'm sure nobody will disagree with a statement like that. During the last couple of years however, we seem to have hit a mid-life crisis of the Internet. The sudden boost of Internet technology over the past decade does not fit well with our outdated design principles for network security. Most organizations hold tight to their fortress approach in trying to protect the internal network from the hostile Internet. Understandable, but not really realistic. In the Netherlands, we are particularly proud of our water management techniques. In a country that lays for more then sixty percent below sea level we know that we have to build and maintain solid dikes to prevent our country from flooding. Having holes in these dikes quickly diminishes the whole purpose of have a dike. The same holds true for perimeter defence in computer networks. Information leakage via email, hyves, my space or mobile data solutions like iPod or USB diminishes the purpose of perimeter security. Today's business world is one of collaboration, one of working together., one of global markets. The Internet is the ideal candidate to support this collaboration. The Jericho Forum (Open Group), formed by Security professionals from the largest organisations in the world described their vision of network de-perimeterization and boundryless Information flow™ in various publications. These visions formed the starting point for Capgemini's Security & Innovation Research Centre.

Together with the best universities in the Netherlands, Capgemini's offers academic researchers and graduate students to ability to conduct empirical academic research into the topic of Collaboration Oriented Architectures or to conduct feasibility studies into the Jericho Forums visions.

Marco Plas

Head of Jericho Research
Capgemini Security & Innovation Research Centre
Capgemini Netherlands

Executive summary

Nowadays the business drivers are changing, businesses want to able to be more collaborative with there partners in order to be more efficient and increase there sales. To do this their information systems must be able to interact and exchange information, but are restricted by their security perimeter. Even when the problem of the security perimeter is overcome other problems are still an issue. Besides technical problems, like how to secure the information and deciding who may access which data, a non-technical problem of deciding if you even want to do business with a certain company has to be made. In order to make a decision a business want to know the trustworthiness of a company. This and more is the focus of the Jericho Forum. The Jericho Forum, as a part of the Open Group, was founded by specialists within these areas that understood these problems. As an solution they created the concept of 'de-perimeterization', which enables companies to create collaboration and commerce over open networks while still being secure. To accomplish this a lot of different areas of security have to be researched, one of these areas is trust. As an participant of the Jericho Forum, Capgemini recognizes these changes within the market, but wanted some practical and workable solutions. It there for created the Jericho Project Group. As one one the members of this group I researched the subject about trust. Trust is needed so that different people and businesses can perform transactions between each other. To define a level of trust four subjects are relevant, these are identity, reputation, behaviour and control. These processes, that are needed to determine the trustworthiness of someone, are implemented in a concept given by my organizational supervisor and the Jericho Forum, that is a Trust broker. This Trust broker will deal with all trust relations with partners, thus will handle all external communications. In order to do this a framework is suggested that will combine all services of the network, so that the Trust broker is suitable for the job but can not control more then two operations within the transactions taking place. The biggest problem that the Trust broker has to solve is the problem of control. This is will be done by a legal framework as suggested by the Liberty Alliance. This framework will give legislative control to the Trust broker by means of contracts. Techniques to monitor these contracts will give the input to determine someone's trustworthiness. Different Trust broker models can be applied within these Legal framework models. The three Trust broker models that are proposed are a central, server/client side and a peer-2-peer Trust broker, each with their own advantages. Closing the essay, the role of the Trust broker within the three different identity models are clarified. And some suggestions plus proposals are given with which technologies a Trust broker can be implemented. The conclusion is that a Trust broker can be made, but not with the present maturity level of the available technologies. But when implemented the Trust broker will become a gateway for expanding trust from the real to the digital world by delivering secure services to the world.

Contents

1. Introduction

Organizations and individuals are depending more and more on the internet. Terms like ‘to google’, ‘you’ve got mail’, or a Dutch example ‘msn-en’ (English; ‘msning’), have found a permanent existence in our life. But also booking a trip, check for opening hours or departure times, we consult the internet. Some companies exist only because of the services they provide on the internet. The internet has accelerated businesses processes and made them more efficiently. The acceptance of internet amongst people and businesses is very high. This fact has got the attention from the criminals which are becoming increasingly more active. The aim of the cybercrime has shifted from the popularity to the financial side. Before hackers were satisfied by defacing a website, now their goal is receiving valuable information which can be sold for large sums of money on the black market. Leaking or losing this sensitive information occurs so often in the U.S. that a law was created to oblige companies to inform the user when such a thing occurs. Because of those problems people and companies tend to get more reserved about eCommerce. And for businesses, depending on the internet, this leads to a drop in sales. In order to continue doing business as usual there must be made some protection against threats from the internet. This security layer against threats is now implemented by means of a firewall. The function of this firewall is to protect against unauthorized access from the internet. A good comparison can be made with the military. In order to protect their base against any outside threat they surround the base with a security perimeter, by means of a fence. The same idea goes for the firewall, where the base is the network, the outside is the internet, and the security perimeter is the firewall. But today the need to communicate with the outside world is constantly increasing. Sharing information with partners around the world is becoming a requisite. In order to make this possible some ‘holes’ must be made within the perimeter to allow the information flow. For each new communication method a new opening is made, until the perimeter has become the digital equivalent of Swiss cheese. So to open up the network to partners the perimeter of the network must disappear. This process is called ‘de-perimeterization’. Taking away the perimeter does not mean that it is not secure any more. An de-perimeterized network should be as secure as a network with a perimeter. To accomplish such an architecture it has to be created with security build into it, not added in the final phase. Such a proposal is given by the Jericho Forum as part of the Open Group. Their vision is to let data secure itself, instead of shielding a network from the world.

2. Aims of research

Aims

The aim of this essay is to research trust in a digital environment, determining the role of a Trust broker in a de-perimeterized network and recommend which are the best open standards and technologies in order to create a Trust broker. To achieve this the following questions will be researched and the answers will be analyzed:

- Determine what trust is
- Determine where digital trust fails
- Determine which fundamentals are needed to improve digital trust
- Determine which basic functions the Trust broker will perform
- Determine which technical implementations can deliver these functions
- A recommendation if the Trust broker can be implemented and with which technologies

Research method

For the research I will use the hourglass model. This model starts with broad spectrum of research and will slowly focus upon the required information. After the focusing it will expand again, leading to the end result. This research will be performed in several phases. Firstly, I will analyze the entire picture that the Jericho Forum has created, by reading the white and position papers. Secondly, I will search to define the main topics, by reading articles and other documents. Thirdly, I will answer the research question in a basic way, by means of logic or theories that I discovered. Fourthly, when answering the research questions I will use or create new concepts. Fifth, after the concepts are clarified, technologies are chosen. These phases will be dealt with in a iterative approach.

Structure

This essay is structured in eleven chapters, including this chapter. Chapters two and three introduce the Jericho Forum and the Jericho Project. Chapter three will provide the different research areas that are done within the Jericho Project. Chapter four covers the businesses case of the Jericho Forum for a de-perimeterized network and the Jericho Forum position about trust & co-operation is described in chapter five. Chapters six and seven explore and describe the Trust broker framework, which functions it comprises and how to fulfill these functionalities. Chapter eight investigates which presently available technologies are suitable to implement the Trust broker functionalities as described in chapter six and seven. Chapters nine deals with the feasibility study of the suggested solutions, and in chapter ten I provide the conclusions and some topics for future research.

3. Jericho Forum

The Jericho Forum is an international group of professionals who are all tackling issues around de-perimeterization. This Forum is managed by the Open Group, the mission that the Open Group wants to accomplish is;
"The Open Group is a vendor-neutral and technology-neutral consortium, whose vision of Boundaryless Information Flow™ will enable access to integrated information, within and among enterprises,based on open standards and global interoperability."[1]
The Jericho Forum was founded by specialists in the UK. They understood that the market was still trying to re-enforce a crumbling perimeter, while other companies were trying to communicate securely without any perimeter to increase flexibility. They knew that if they want to come up with solutions they first had to properly define the problem between business drivers and security.

"Jericho Forum aims to develop and influence information and communications technology (ICT) security standards. These will facilitate the secure interoperation of ICT to support collaboration and commerce over open networks, within and between organisations, based on a security architecture and design approach entitled de-perimeterisation."[2]
De-perimeterization stands for the act of taking away the fence around the network. And instead of only guarding the perimeter security measures will focuses the attention on the most important parts, starting with the data itself. Data should be able to protect itself against any threat. The Jericho Forum specialists have made it their mission to become a catalyst in the realization and development of the de-perimeterization concept. They are trying to do this by sharing their knowledge by writing white and position papers. These papers discuss issues like; Architecture, Trust & Cooperation, Encryption, Secure Protocols, Wireless, VOIP, Federated Identity, et cetera.

The Jericho Forum co-operates with many different partners. It comprises academies and the public- & commercial sector. All these partners understand that the way the network is secured today is not sufficient and it can not be combined with the new business models that are created today. These new business models get their profit out of the following subjects:

- Increasing online business by collaboration with several partners, by which it must be possible to share sensitive data or trade secrets with each partner
- Be able to outsource and offshore any supporting service, core-business and supporting capabilities globally
- Be able to use low-priced open networks for commerce and business

1 http://www.opengroup.org/ accessed May 2007.
2 https://www.opengroup.org/jericho/vision_wp.pdf Vision Paper accessed February 2007.

4. Jericho Project

After repeatedly hearing the same kind of problems from different large companies, Capgemini has decided to start preparing for these possible huge opportunities by starting a innovation project. The mission of this project is to give the vision of the Jericho Forum a pragmatic view and some feasible implementations. By doing this Capgemini entered a small group worldwide that actually engaged this subject, certainly within the Netherlands. This initiative was taken and leaded by Marco Plas. Marco has become a specialist, or to some a guru, during the last 15 years in the areas of risk management, information security and all related subjects. The first research group that he has put together exists in a set of five students, where each student deals with a specific part of the Jericho Forum and will do this with its own specialism.

Jericho Project Research Area	Jericho Project member
Authentication	Evgeny Barannikov
Authorisation	Leon Teheux
Accounting	Evgeny Barannikov
Endpoint Security	Leon Teheux
Data classification & Information leakage	Remco van Marle
End-to-end encryption	Alina Stan
Trust broker	Adriaan Bruning

Initially the aim of the project was to produce a prototype and deliver it around august, so we could compete in the Jericho challenge. Unfortunately this challenge was cancelled due to the rearranging of prize money that would have been funded by the U.S. Army. Nevertheless the research at Capgemini continued but is more directed towards a theoretical- then practical research.

The Jericho Forum Commandments

To give researchers a sense of direction the Jericho Forum defined the areas and principles that must be observed when creating solutions for a de-perimeterized network.These commandments serve as a benchmark for the new concepts and solutions that this research group will develop.

Jericho Forum Commandments[3]

1. **The scope and level of protection should be specific & appropriate to the asset at risk.**
   The new architecture must enable business agility. In order to provide this protection must be located closer to the assets.
2. **Security mechanisms must be pervasive, simple, scalable & easy to manage.**
   Complexity must be avoided. Multiple security mechanisms have to be interoperable to provide the scalability that is needed to span all tiers in a network.

3 Extracted from http://www.opengroup.org/jericho/commandments_v1.2.pdf accessed May 2007

3. **Assume context at your peril.**
   When implementing security solutions it is important to know the limitations of the environment and to known problems with the solution, in order to survive in a hostile world.
4. **Devices and applications must communicate using open, secure protocols.**
   Security requirements should be build in from the start, not added-on. To ensure a wide acceptance and a thorough review security protocols have to be open and not obscure.
5. **All devices must be capable of maintaining their security policy on an untrusted network.**
   Security policies must be able to protect their assets in any context. Devices must be made capable to maintain their policy on any network, even the internet.
6. **All people, processes, technology must have declared and transparent levels of trust for any transaction to take place.**
   Trust must be applicable to any entity. Trust in the context of a de-perimeterized network is about establishing transactions between contracting parties. To do this an understanding and monitoring each others obligations is necessary.
7. **Mutual trust assurance levels must be determinable.**
   Entities must be capable to acquire appropriate levels of mutual authentication in order to access systems and data.
8. **Authentication, authorization, and accountability must interoperate outside of your area of control.**
   By means of the AAA framework the capability to created only one instance for entities must be made possible. To support these instances across several domains, systems must be able to pass on security credentials.
9. **Access to data should be controlled by security attributes of the data itself.**
   Data must be capable to use several attributes that contains information about the confidentiality level. These attributes have a temporal component and can be held within metadata. Security measures can be implemented using encryption.
10. **Data privacy (and security of any asset of sufficiently high value) requires a segregation of duties.**
    In order to prevent a top in the chain of trust all important processes must fall under independent control.
11. **By default, data must be appropriately secured when in stored, in transit and in use.**
    Data should be able to protect itself within each state. However not all data has to be secured.

These commandments created the requirements to develop a new approach. Each member defined the processes necessary for this new approach. The connection of these processes has lead to the result given in the figure 1.

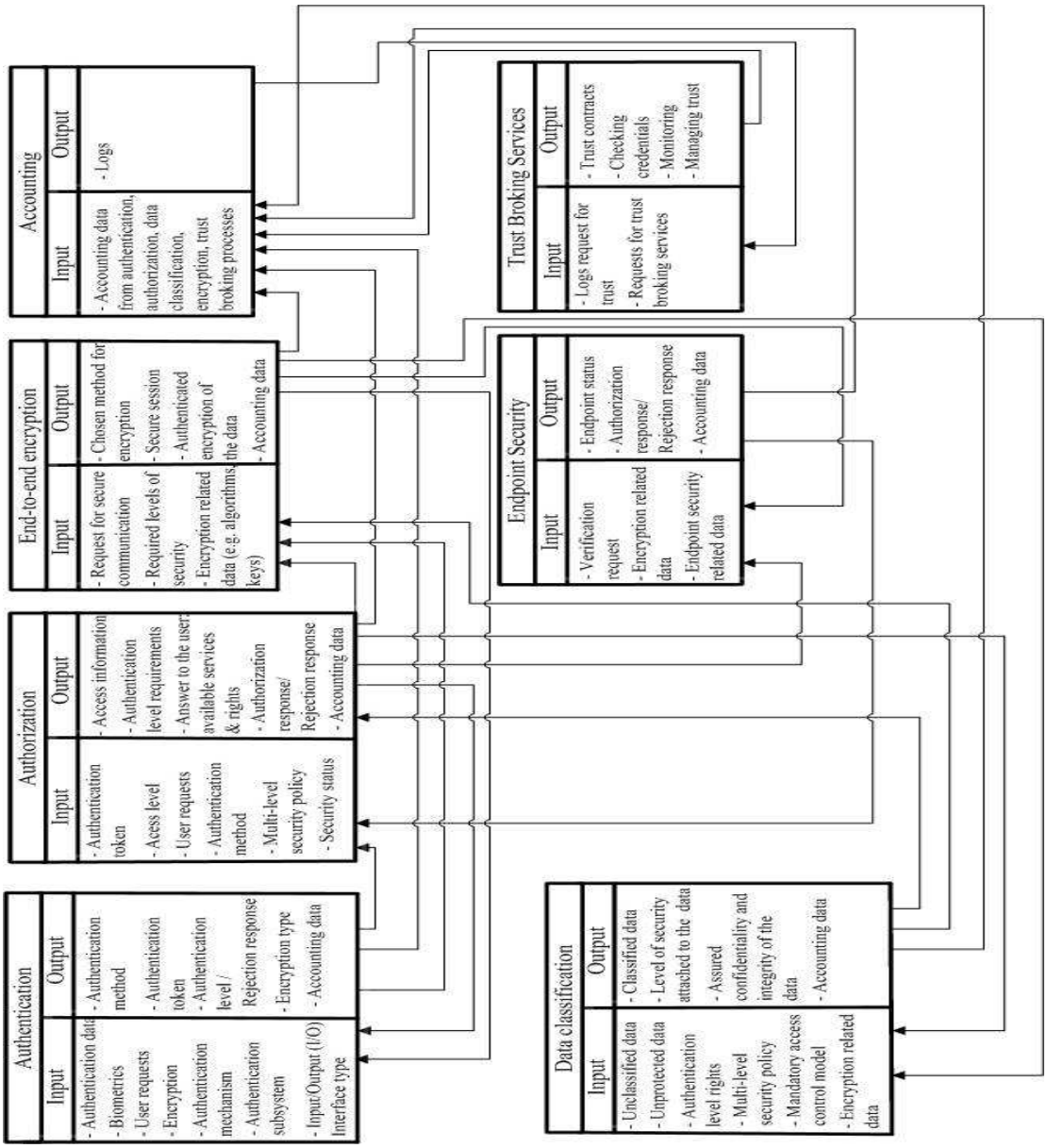

Figure 1: Jericho Project dependencies

AAA framework

Authentication

Authentication is the process that establishes a subject's identity. It plays a very important role in the Jericho Project. Successful authentication will allow a entities to initiate data transactions. Authentication can use a single or multiple factors. The more factors are present the more assurance one receives of the person's identity. According to the Jericho Forum Commandment number 8 "Authentication, authorization and accountability must interoperate outside of your area of control", identity data must be not usable only within one domain, but also be inter-exchangeable among multiple parties. The aim of the research is to identify the methods and technologies with which a user can be authenticated in federated and user-centric identity systems. Authentication is interconnected with every other part of the Jericho Project research. Authentication delivers identifying information, which is necessary to perform other processes. Authorization needs this identity data to determine access rights. Accounting keeps logs of all the authentication process for the further auditing or investigation. Some identity data may also be used by the encryption process to encrypt either authentication or data transaction. (Source: E. Barannikov)
Figure 2 displays the connections authentication has with all the other processes.

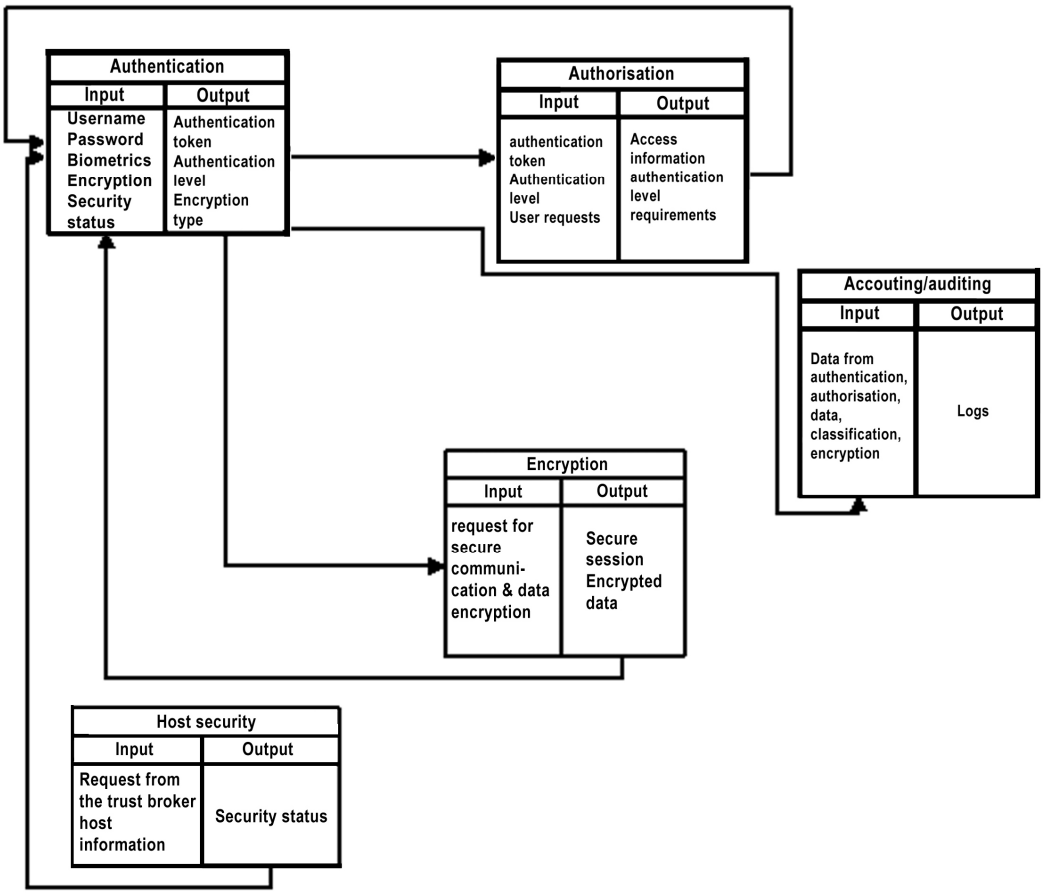

Figure 2: Authentication dependencies within the Jericho Project

Authorization

The Authorization process enables the enforcement of rights to information and services. The process is to establish the rights of the entity in association with a set of resources. Prior to authorization the process of authentication is needed to establish the credentials of the entity. After the identity of an entity is validated a entity can try to access a specific resource. The authorization process will allow or deny the request. The decision will be based upon the rights required to access the resource, and the rights a entity has concerning the resource. As such, Authorization research topic is an essential part of the Jericho Project. Without authorization, no controlled network interactions can exist. A new architecture that can add flexibility and interoperability to this concept is needed. The claims-based architecture is a promising example. Whereas until now users had to provide proof of identity before the authorization process could commence, authentication and authorization can be combined to provide a flexible and more effective solution. In the context of Jericho Project, the research about authorization has several interactions with other research topics. The Authentication process needs to authenticate entities before authorization can take place, whilst the accounting process needs to gather data and process it. In addition, the Endpoint security process may need to deliver information that can be used to determine authorization rights. (Source: L. Teheux)
Figure 3 displays the connections of authorization with the other research topics.

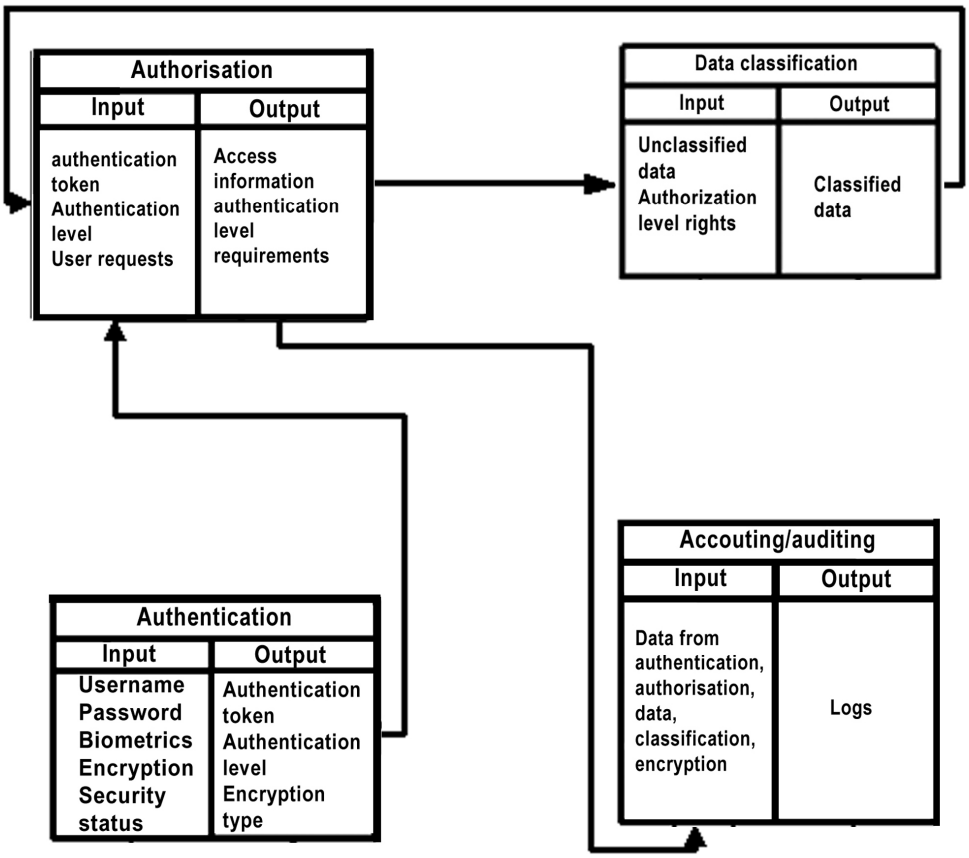

Figure 3: Authorization dependencies within the Jericho Project

Accounting

Auditing is a process that collects and processes the log data, which is delivered by other processes. Separate IT systems in the enterprise architecture provide log data, which is processed independently from each other. In case of security breach or performance analyses multiple logs must be accessed and analysed. Auditing policy must comply with the legislation of the country, where the company is established. Also log retention period is dictated by the security policy of the corporation and the laws of the country. Auditing process may deliver data to other processes that can determine, through certain algorithms, the trustworthiness of the authenticated party. This data may also be accessed by the third party that objectively and independently establishes the entity's reputation. Anonymity is a very important factor here. Not all data may be disclosed to other parties. The goal of this sub-project is to research and define technology which could consolidate the logs from the multiple systems and provide certain log data to other processes. (Source: E. Barannikov)

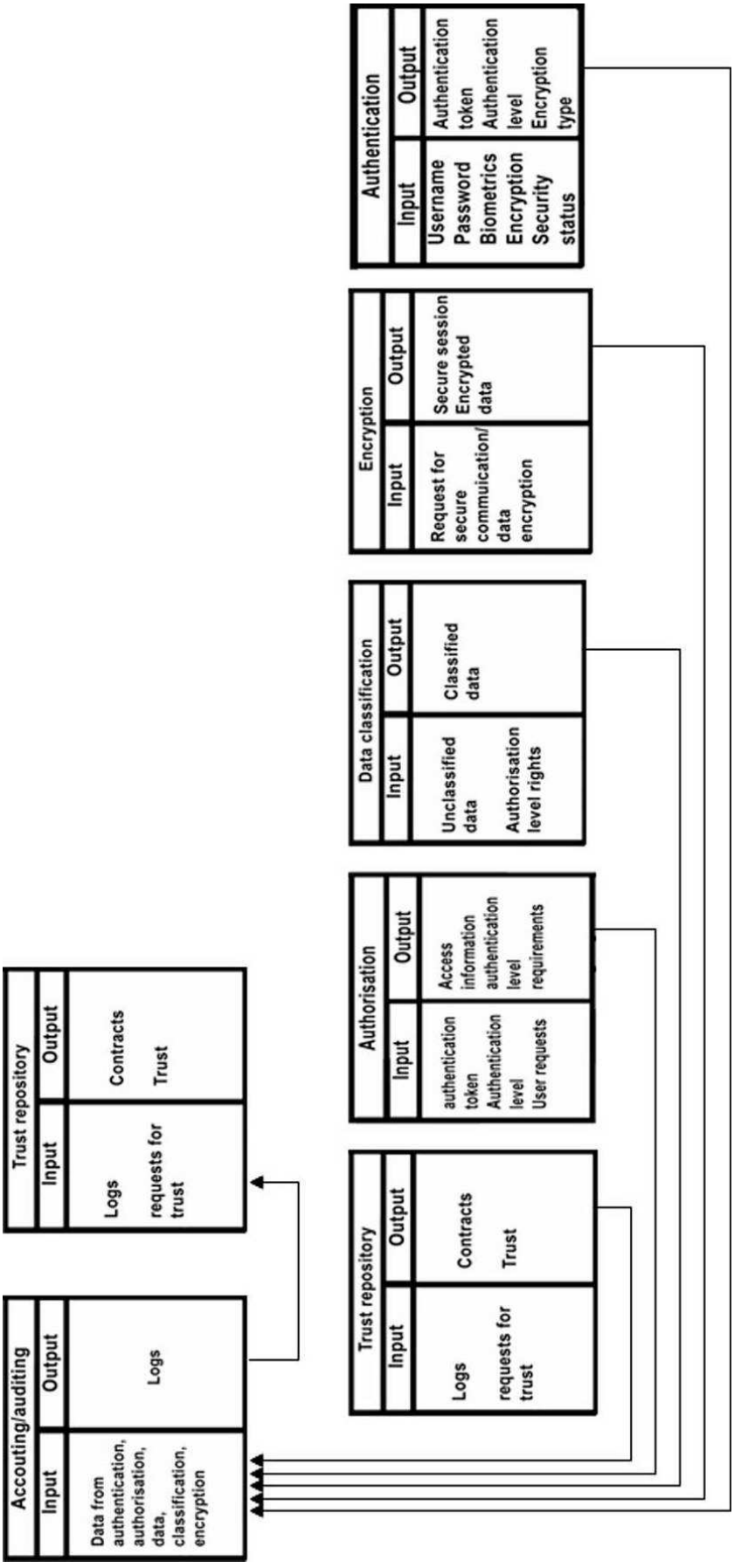

Figure 4: Displays the connections of accounting process with the other research areas.

End-to-end security

The Endpoint security process is responsible for providing the means to establish inherent trust levels between endpoints. In order to establish these essential trust levels endpoint security must create a situation where all the devices involved within a transaction meet the criteria of trust for that transaction. At the moment, many Endpoint security or Network Access Control solutions exist. However, most of these solutions were not designed to interoperate with other solutions and they lack the ability to verify all network devices. Most solutions provide only Endpoint Security for PCs running certain Operating Systems. Several Jericho Forum Commandments refer to the Endpoint Security process:

- Jericho Forum Commandment number 2 states that *"Security mechanisms must be pervasive, simple, scalable & easy to manage"*
- Jericho Forum Commandment number 5 states *"All devices must be capable of maintaining their security policy on an un-trusted network"*
- Jericho Forum Commandment number 7 states that *"Mutual trust assurance levels must be determinable"*

These commandments require a solution where every device connected to a network should be able to participate in the Endpoint security process. This means that a universal standard should exist that governs agent behaviour and interactions. For enabling secure devices to function in a possibly insecure network, these must be able to maintain their security policies. Consequently, this implies the existence of a solution that can monitor devices' status, can act upon it, essentially requiring agents installed on devices. Endpoint security research topic is interconnected with several other research topics within Jericho Project. The Authorization process within Jericho network will be dependent on the Endpoint security process for providing authorization information. In addition, in Jericho networks, the Accounting process will be used to handle information gathered by the Endpoint Security process. (Source: L. Teheux)
Figure 5 displays the connections that Endpoint security has with the other research topics.

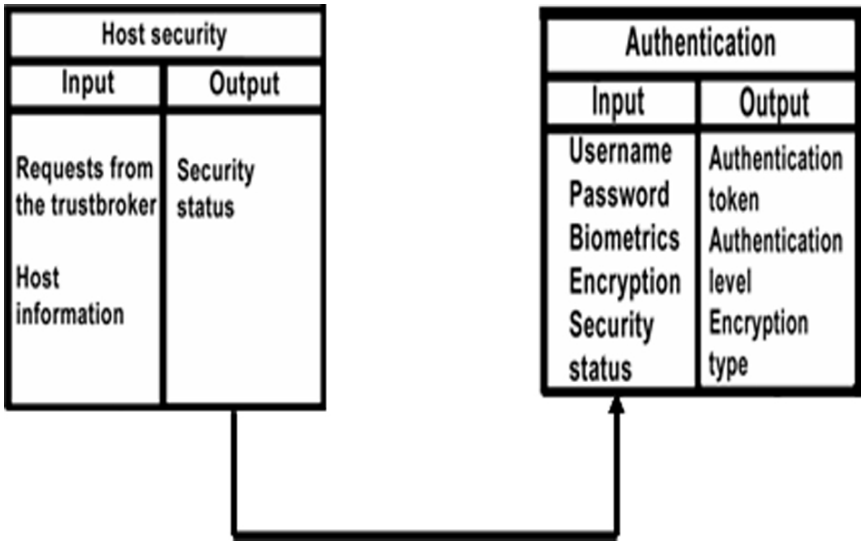

Figure 5: Endpoint security dependencies within the Jericho Project

Data classification

Data classification is the process that provides data with the protection against access from unauthorized entities, by means of encryption or other security measures. As indicated by the Jericho Forum there is a need to find an ideal way to classify data in order to prevent information leakage. The Jericho Forum Commandments that make this need clear are:

1. *"Access to data should be controlled by security attributes of the data itself"*
2. *"Data privacy (and security of any asset of sufficiently high value) requires a segregation of duties/privileges*
3. *"By default, data must be appropriately secured when stored, in transit and in use"*

In order to comply with the Jericho Forum Commandments certain steps have to be taken: Firstly, the data should be encrypted in order to keep entities, that do not yet have the corresponding access level or that are not authorized, from outside the area of control. Secondly, entities who want to access the data have to be authorized. This can be done by the author of the data, but this way it is too time consuming. It will be easier for the author to attach a group-status to the data e.g. public, non-confidential or confidential. Group-status are agreements like, who may access the data, and what the level of encryption must be. Thirdly, to maintain data privacy, data will require an authentication level. Then the data can only be accessed by when a entity is identified and authorized. The aim of the Data classification area is to research ways how data can be classified automatically in order to secure itself. (Source: R. van Marle)
Figure 6 displays the connections of Data classification with the other processes.

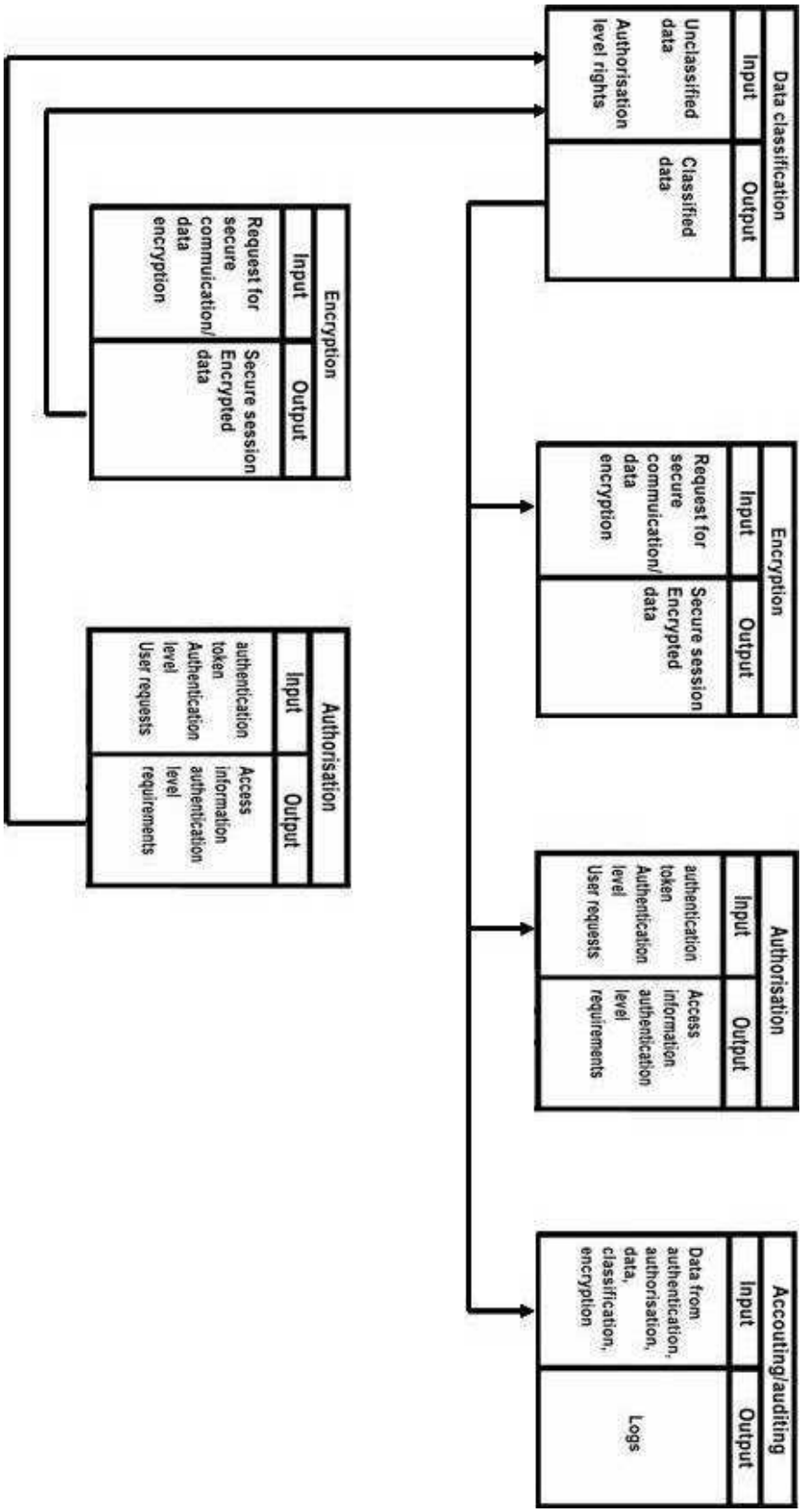

Figure 6: Data classification dependencies within the Jericho Project

End-to-end encryption

End-to-end encryption focuses to achieve authenticated encryption for data in transit. Within the context provided by Jericho Project, end-to-end encryption will explore and propose valid solutions to ensure the integrity and confidentiality of the data in transit. Apart from privacy and integrity, for achieving secure communications other requirements have to be fulfilled as well: establishing a secure channel, the entities need to be authenticated, the source of the messages have to be authenticated as well, non-repudiation, accountability. The starting point for end-to-end encryption research is based on Jericho Forum Commandment number 4 that states the following: *"Devices and applications must communicate using open, secure protocols"*. Steps to be followed for secure communications In order to provide end-to-end encryption for the data in transit, in the context of Jericho Project, a number of steps have to be followed. Firstly, the entities involved in the communication have to be authenticated in a handshake protocol. Secondly, there will be established a secure connection between the entities, and a secure session will be set up for transmitting the content securely. This step is being performed or not, according to the output of authentication, authorization processes. Then, the adequate cryptographic primitives are chosen for achieving, further in the communication process, certain security services (e.g. confidentiality, integrity, authentication of the source of messages, non-repudiation). Also, the most suitable ways of distributing the keys are chosen and an agreement is reached. Typically, the publickey algorithms are used for secure key exchange, while the symmetric-key algorithms are used for encrypting the data in transit. Moreover, for the research on end-to-end encryption in the context of Jericho Project, the sources of the transmitted messages are authenticated, so the aim is to achieve authenticated encryption for data in transit. (Source: A. Stan)

Figure 7 displays the connections of End-to-end encryption with the other research areas.

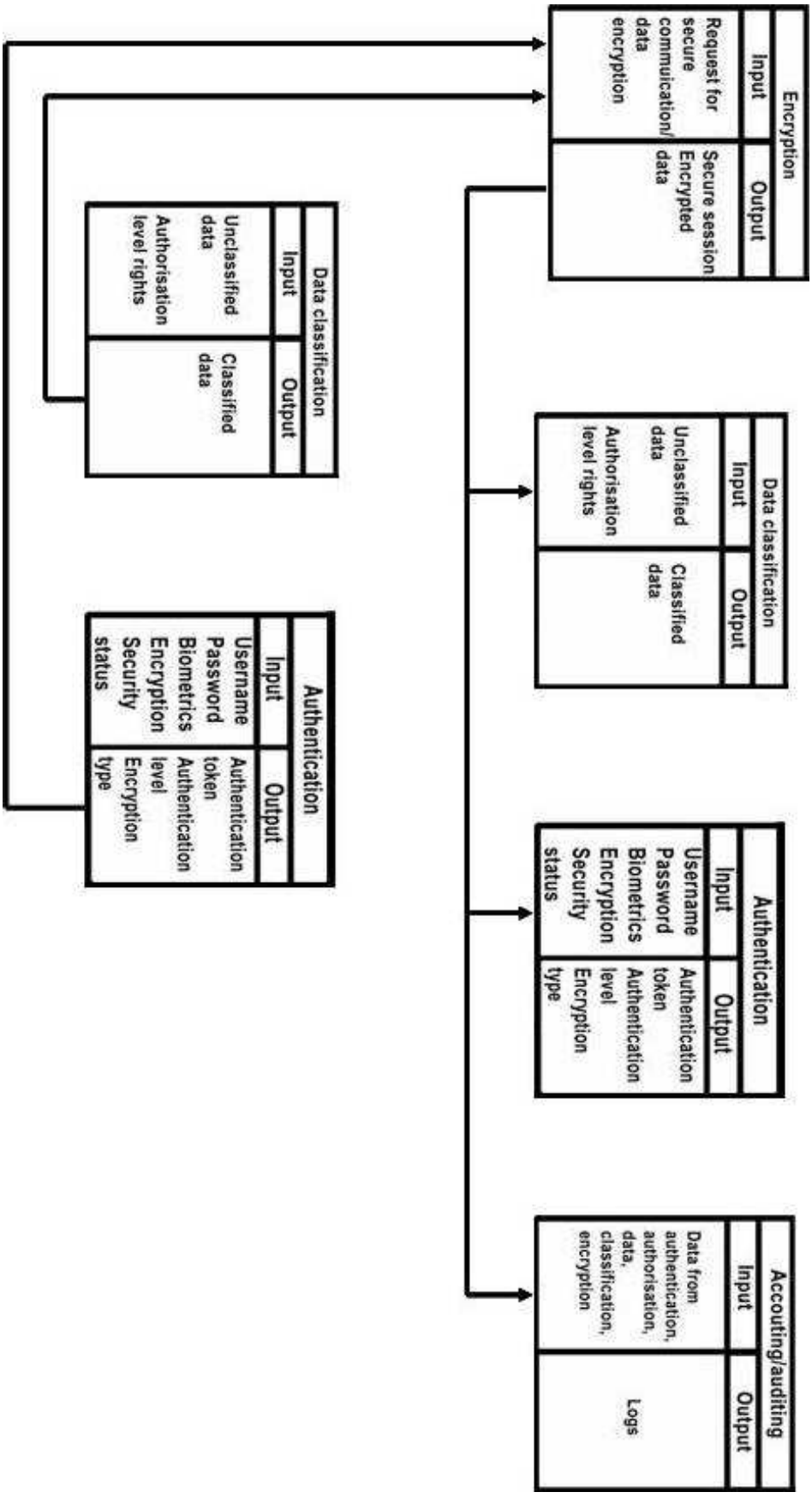

Figure 7: End-to-end encryption dependencies within the Jericho Project

Trust broker

The main purpose of the Trust broker, within the context of the Jericho Forum Project, is that it will act in trust. To do this the Trust broker will establish and manage trust between parties. It will do this as a neutral third party that will facilitate certain services from which it can not take any advantages, except some compensation from the two or the several other parties. These services can take place on all kinds of areas because the service, or data which originate from the service, is frequently carried out at one of the acting parties. Things the Trust broker will supervise are; if these parties can trust each other, if these services are carried out effectively, if it is even possible to carry out these services, and further if they are dealt adequately. This means that a Trust broker will act between two or several parties who want to be able to do business with each other, but need an extra factor of confidence to establish this. For this, the Trust broker must determine if every party can be trusted and if it is still the same party when the agreement was concluded. Therefore, in principle, the Trust broker creates a Circle of trust between these two or several parties. To resolve or reduce cybercrime problems surrounding digital trust will be a one of the main goals to achieve. In order to accomplish this, there must come some kind of simple and unambiguous trust system. In short, to reduce the crimes in the digital realm it is necessary to have a system that can measure or define someone's trust level. The main goal of this research is to establish trust levels and to define the actions of a Trust broker within the context of the Jericho network.

Figure 8 displays the connections of the Trust broker with the other research areas.

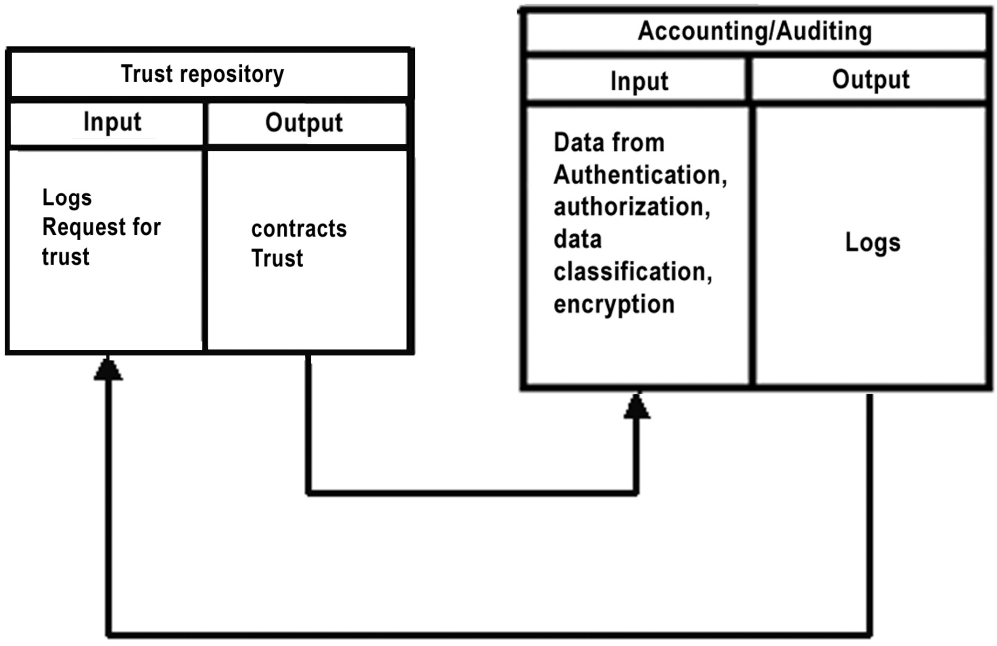

Figure 8: Trust broker dependencies within the Jericho Project

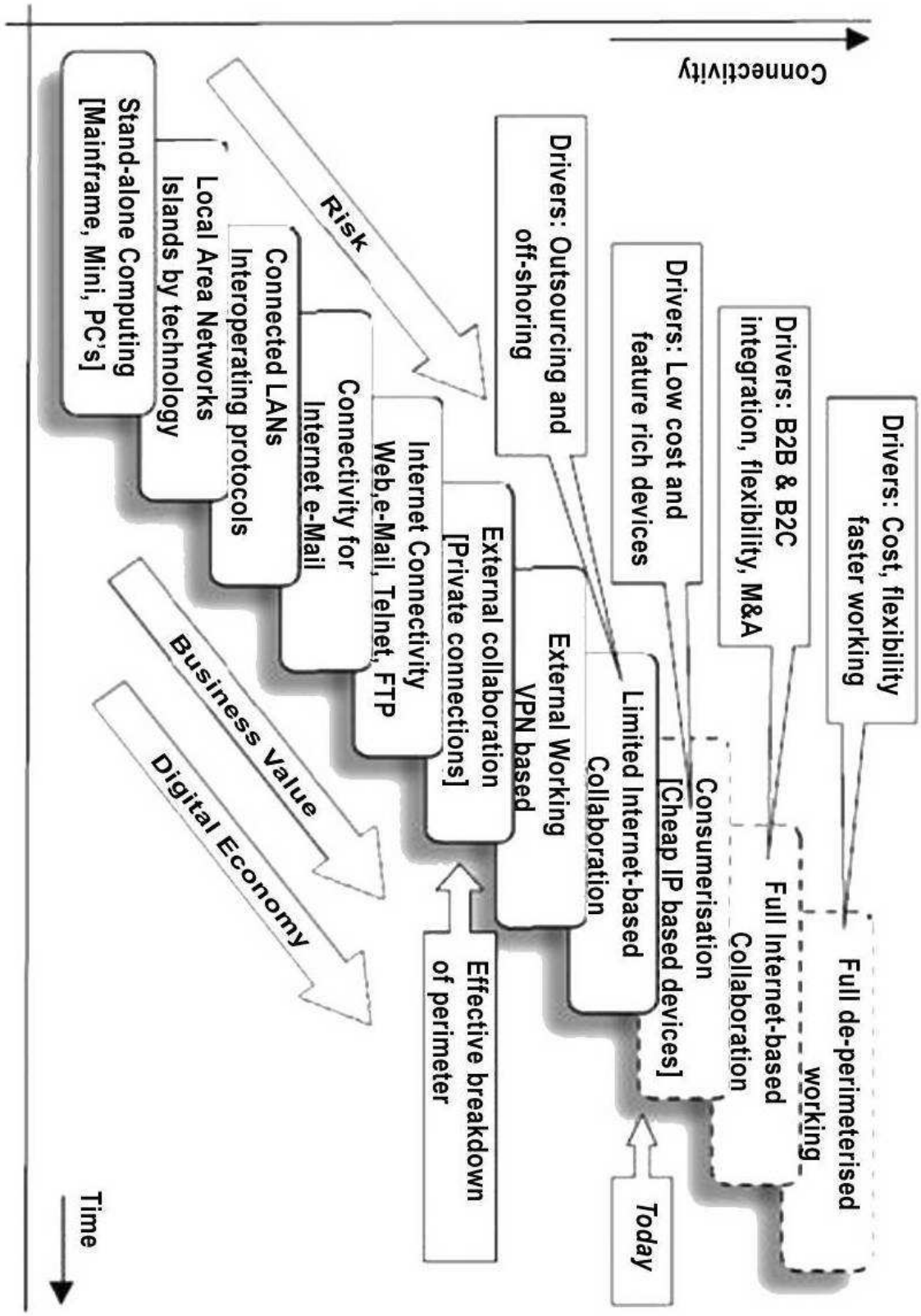

Figure 9: Business rationale for de-perimeterisation (adopted from Business case Jericho Forum)

5. The business case of the Jericho Forum

In order to make the 'de-perimeterization' concept more tangible for businesses the Jericho Forum made a Business Case White Paper[4] where they explain the need for change from a business perspective. Here is a short summary. Computing history can be defined in terms of connectivity, it began with no connectivity and developed into restricted connectivity. Restricted because of perimeter that is obstructing private connections. Today every organization is experiencing a change in the way they are doing business, key indicators are:

- integration between the legal business border and the network perimeter
- B2B relationships are demanding to connect systems directly
- Shared applications across business relationships
- Increasing number of applications using technology that bypasses the firewall

These indicators are suggesting that most of the network security perimeter is disappearing. However still many people, including business and IT leaders, think that good security starts and end with a hardened perimeter. But what they do not realize is that the perimeter is inhibiting innovation, wide collaborative working, expansion and speed to market. De-perimeterization will enable new ways of working; probably unimagined or considered and dismissed by the businesses. Without the hindering perimeter new ways of working can be quickly and cheaply implemented.
Until recently most device and network security had been added over time. But new technologies realize that good security only occurs when it is build-in or when it provides 'defense-in-depth'. A trend that is occurring is that organizations are implementing security 'zones' by shrinking their perimeter (or micro-perimeterization). This can help an organization to make the step to de-perimeterization. But in itself it can not be the solution, because in wide-spreaded it adds network and management complexity, points of failure, and bottlenecks for network traffic. Thus it is not very viable in the long term.

"De-perimeterisation requires security to be at the heart of the organisation's distributed technology architecture; consistently implemented in end-user devices, application services, and surrounding the organisation's critical information assets themselves. Thus reinforcing what has been known for years but rarely implemented, that unless security is built-in from the ground up it will rarely be effective."

De-perimeterization will be like a natural evolution of the network and shall not change overnight. During this slow transition alternative security measures will be implemented, such as micro-perimeterization. Fortunately de-perimeterization technologies can easily co-exist in a perimeterized environment, which will aid the transition.

4 https://www.opengroup.org/jericho/Business_Case_for_DP_v1.0.pdf accessed May 2007.

"*De-perimeterisation is simply the concept of architecting security for the extended business boundary and not an arbitrary IT boundary. It is not a solution in itself; however de-perimeterisation, properly implemented, is a set of enabling technologies that promises to:*

- *Reduce complexity by unifying and simplifying solutions, and generally reduce cost,*
- *Enable business flexibility, cost-effective bandwidth and infrastructure provision,*
- *Provide increased security thereby reduce business risk,*
- *Enable multi-vendor outsourcing, simply and effectively,*
- *Provide a simpler and thus more auditable environment,*
- *Provide true defence in depth, from network through to the actual data."*

6. The position of the Jericho Forum about Trust

To support the business case, the Jericho Forum made some interesting position papers about several subjects concerning 'de-perimeterization'. These subjects are:

- Architecture
- Protocols
- Voice over IP
- Wireless
- Internet Filtering & Reporting
- End Point Security
- Trust & Co-operation
- Federated Identity
- Information Access Policy Management
- Principles for Managing Data Privacy
- Enterprise Information Protection & Control (Digital Rights Management)

Since the subject that I will research in this essay is about trust and determining which technologies can be used in the creation of a Trust broker, the position paper about Trust & Co-operation[5] interests me the most. The position paper gives an overview of the existing problems surrounding trust and co-operation, why we should care, a background and a recommendation for possible solutions. This paper is very focused on the business to person (b2p) and business to business (b2b) market. As they say the problem today is a friction that resists the growth of eCommerce. It is difficult and expensive to register and verify every identity. A eCommerce company needs to know who the other party is. In order to make an transaction they need to determine the level of trust that is required. "*Trust, in this business context, relies primarily upon contracts (to specify the behaviour that is required) and an enforcement mechanism (to punish and deter non-performance).*" Automating these contracts mechanisms is difficult and expensive, this friction that is reducing the growth of eCommerce. In order to improve this problem the Jericho Forum believes that effective trust management is important in securing electronic transactions involving multiple organisations. And it proposes the creation of a 'trust broker' to handle an organisation's trust relationships. According to the Jericho Forum the most important part of the definition trust is the idea of a contract. This contract does not have to be a legal written contract, it can also be some informal behaviour code within a community. These contracts clearly define the way parties should behave, and give them an accountability mechanism for handling failure of a party. This accountability mechanism can include measures such as criminal prosecution or disciplinary action. But in order to perform these actions the identity of the failing party must be known, so this is an important task of the Trust broker. The Jericho Forum finds trust vital for co-operation among people and organisations. They say it allows two parts of a transaction to be separated in time.

Today these transactions and interactions between people and organisations are increasingly being performed digitally. This creates processes like:

- Authentication, the link between an electronic agent and a real world identity
- Authorisation, determines the rights associated with an entity

5 https://www.opengroup.org/jericho/trust_coop_v1.0.pdf accessed May 2007.

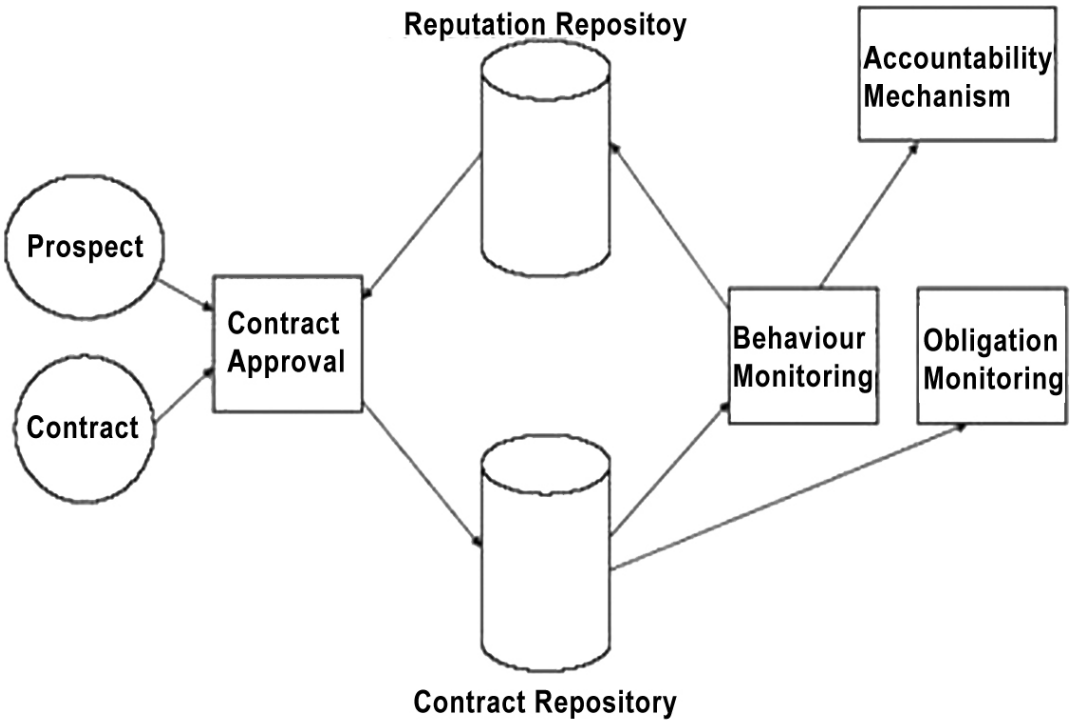

Figure 10: Trust architecture according to the Jericho Forum (adopted from Jericho Forum Trust positioning paper)

As digital interactions evolve, organisations will increasingly be establishing contracts trough the digital way. But in order for this to work organisations will need to understand each others contracts, preferably in an automated way. So that even when the contract is made the accounting continues, and the organisation will have a clear picture of their obligations. How this contract is made depends on how much the parties trust each other. It must decide if the party is trustworthy or not, based on the proposed contract and the perception of the other parties past performance. In order to check this there must be some kind of reputation system, that shows some attributes to the interested party. The trust architecture that the Jericho Forum has created is illustrated below.
In this architecture a business enters an agreement with another party, the prospect. To make a well informed decision (contract approval) the company will use information from the Reputation Repository. This Reputation Repository stores all known information of the other party, their attributes and past behaviour. If the contract is approved and signed it will enter a contract repository so the company can monitor its assets and liabilities. In many organizations this is implemented as a group membership in an user directory. While the contract is being executed by the two parties, two separate functions will determine if the company itself is complying with it obligations (Obligation Monitoring) and the other function will check if the trusted party is complying with the contract (Behaviour Monitoring). This system can work by implementing access management, provisioning and user audit. In case that the other party is not complying with the contract an Accountability Mechanism is invoked to enforce the other party to comply. To make the above model work in a de-perimeterized world it should be generalised, because the model now only supports a person or a single company. To do this, the Jericho Forum thinks that two different points should be addressed:

1. Sharing reputation information between organisations, by:
    a. Direct mechanisms such as federation
    b. Introduction protocols, whereby one party can recommend someone to a third
    c. Market-oriented reputation services such as Experian*
    d. Peer-to-peer mechanisms, where the eBay feedback system uses it partially*
2. Improved mechanisms for delegating contracts.The key challenges, according to the Jericho Forum, are:
    a. Standardising authorisations between organisations
    b. Develop software en services to link identities and authorisations between organisations
    c. And linking the agreement of a contract with provisioning it automatically

7. Research Question: What kind of role does a Trust Broker have in a Jericho Network environment?

To answer this question, we need to establish the definition of trust, what is trust?

What is trust?

According to the online oxford dictionary trust is:

1. *firm belief in the reliability, truth, ability, or strength of someone or something*
2. *acceptance of the truth of a statement without evidence or investigation*
3. *the state of being responsible for someone or something*
4. *law an arrangement whereby a person (a trustee) is made the nominal owner of property to be held or used for the benefit of one or more others*
5. *a body of trustees, or an organization or company managed by trustees*

I will expand upon the first definition. This is two folded because the first refers to a firm belief, thus an emotional act, and second reliability which is a quality that can be measured and therefore a logical act. So trust can be separated in two human acts; emotional and logical. Now that we have established the basics of trust, we can continue to ask the next two questions:

1. What is trust not?
   In a Identity Management white paper written by the Drs. S. Slone and the Open Group Joint Work Area:
   "*It is useful to remember some things that trust is not. Trust is:*
   a. *Not transitive (cannot be passed from person to person)*
   b. *Not distributive (cannot be shared)*
   c. *Not associative (cannot be linked to another trust or added)*
   d. *Not symmetric (I trust you does not equal you trust me)*
   e. *Not self-declared (trust me – why?)*"[6]
2. How do we influence trust so that we can establish or build a relationship with someone, so how can we build trust?

"*Our trust in another individual can be based upon our evaluation of their ability, integrity, and benevolence. That is, the more we observe these characteristics in another person, the more our level of trust in that person is likely to grow.*

- *Ability refers to an assessment of the other's knowledge, skill, or competency. This dimension recognizes that trust requires some sense that the other is able to perform in a manner that meets our expectations.*
- *Integrity is the degree to which the trustee adheres to principles that are acceptable to the trustor. This dimension leads to trust based on consistency of past actions, credibility of communication, commitment to standards of fairness, and the congruence of the other's word and deed.*
- *Benevolence is our assessment that the trusted individual is concerned enough about our welfare to either advance our interests, or at least not*

6 http://www.opengroup.org/projects/idm/uploads/40/9784/idm_wp.pdf accessed March 2007.

impede them. The other's perceived intentions or motives of the trustee are most central. Honest and open communication, delegating decisions, and sharing control indicate evidence of one's benevolence. Although these three dimensions are likely to be linked to each other, they each contribute separately to influence the level of trust in another within a relationship. However, ability and integrity are likely to be most influential early in a relationship, as information on one's benevolence needs more time to emerge. The effect of benevolence will increase as the relationship between the parties grows closer." [7]

If we categorize these three characteristics in the two human acts of trust, emotional or logical, we can see in what degree we can measure a trust relationship. Ability says something about what a person can do or knows, so in general it can be measured and is therefore a logical act. But not all things that somebody knows or can do are specified somewhere so ability can also be an emotional act. Integrity is largely specified by the past actions of the trustee and can therefore also be measured, thus a logical act. For a certain degree benevolence is given by the intentions and motives of the trustee, but these behaviours are determined during a period of time. These intentions and motives can not be measured objectively but the overall conduct can be measured. It therefore is partially a logical act. This categorization shows us that more then 50% of a trust relationship can be measured. The remainder percentage depends on the person itself and how it perceives the relationship.

How do we maintain a trust relationship?

"At early stages of a relationship, trust is at a calculus-based level. In other words, an individual will carefully calculate how the other party is likely to behave in a given situation depending on the rewards for being trustworthy and the deterrents against untrustworthy behavior. In this manner, rewards and punishments form the basis of control that a trustor has in ensuring the trustee's behavioral consistency. Individuals deciding to trust the other mentally contemplate the benefits of staying in the relationship with the trustee versus the benefits of 'cheating' on the relationship, and the costs of staying in the relationship versus the costs of breaking the relationship. Trust will only be extended to the other to the extent that this cost-benefit calculation indicates that the continued trust will yield a net positive benefit." [8]

This implies that we constantly recalculate the relationship (conscious or subconscious). With each change or event within the relationship we evaluate the trust relationship and decided if it is still beneficial to us. The thing that drives us to continue a trust relationship is the possible punishment that can be expected if we break it or the possible reward if we continue the trust relationship. So maintaining a trust relationship depends on whether or not it is still beneficial to both parties or at least one of them. Methods to manage or control the relationship are given in the form of rewards and punishments.

A brief summary; what are the basics of trust? A trust relationship is build upon a logical and emotional act, measured by the ability, integrity and benevolence of somebody.

7 http://www.beyondintractability.org/essay/trust_building/ accessed in February 2007.

8 http://www.beyondintractability.org/essay/trust_building/ accessed in February 2007.

Maintaining a trust relationship is done by continuously measuring these characteristics and evaluate if the relationship is still beneficial and or reliable.
Now that we have dealt with the very basics of trust (what it is, how to build it and how to maintain it) we can examine what digital trust should be like.

What is digital trust?

In essence digital trust is the same as trust in the real world, only the manner how it is done is different. I will examine what this difference is and how we can change this. What are the main actions of trusting somebody in the real world? This depends on the sort of action you are performing. In case of a verbal agreement a person will not take a high risk, unless he knows the person already and has established some kind of ability and integrity reputation of each other. If this person will do it in a more official manner he will make a contract that both parties must sign and let them prove their identity with some sort of passport. In high risk situations you can perform checks of someone's identity, their abilities and past actions. By means of a contract companies can mitigate their risks, because if the other party does not fulfill his end of the bargain a company is legally authorized to handle accordingly.
In short this means:

1. You always want to know who the other person is,
2. You want to know specific history details of the person to perform a some kind of risk management, e.g. financial records or a reference by somebody else,
3. You want some methods to manage the trust relationship so you can reduce the risk you are taking, e.g. contracts and signatures.

How can these processes be performed in a digital environment?
The first point is done by authentication; the second point can not be performed without the help of somebody else with the appropriate access. The third point can be done with digital contracts and digital signatures but these are not yet legally recognized. So we can conclude that digital trust as it is now doesn't work.
Evidently the basics of trust are not fully implemented in a digital environment. Let's analyze this:

1. Who is the person you want to build a trust relationship with? In order to do this in a digital environment you will need some sort of verification and authentication process. Authentication services are widely provided but they can not guarantee if the information about the user is correct, it can only check if it is the same user again (unless the account has been hacked),
2. How can ability, integrity and benevolence be measured in the digital realm? In order to do this you must have a authority to check this private and sensitive information, and tells whether it is the truth or not. All of these functions are not widely provided and if they are provided you can not check if the source can be trusted,
3. How is it possible to constantly evaluate the trustee and check whether or not things have changed that you don't like? How can you be certain if you trust someone without breaking his privacy? One way to do this is to use the system for measuring ability. But when that system is used you must

know how often this measurement takes place or you must be able to perform it your self,

4. How can you control and manage the trust relationship, without legislative support? A trust relationship without the tools for control and management can not hold very long, the law is probably the most important control mechanism.

What has to be done in order to make digital trust work?
As most things in life, there is not one simple answer to this question. Instead it is divided in several subjects. The central one is identity as everything else around trust is based on someone or something identity. If you don't know who or what somebody is, how can you know what his abilities are? After you know someone's identity you must be able to check this information, how else can you otherwise be certain if somebody is who he says that he is. Second, once you know for certain that the identity is true, it depends on what kind of trust relationship you want to establish with this identity. If there are some high risks, you probably want to know everything that this person has ever done, but if there are no risks you don't need to know so much about the other person. Third, after you know what you want to know you have to be able to be informed if something changes or at least be able to check this information whenever you like, for as long as the trust relationship exists. Fourth, the law must become active at this point because without proper control mechanisms, not many people will find it necessary to oblige. This is due to the nature of people. This is hard to explain, but some people just want to disobey and others just want to see what will happen if you don't oblige. There is no apparent reason why this is done, but the fact remains people do not always obey the rules. So, to make digital trust work there must be done something about four different issues, identity, ability, additional information or integrity and legislation, starting with identity.

What could a Trust broker be?

If digital trust starts with identity there must be some kind of trusted place where you can store your private sensitive information without worrying that this information will be lost or misused. How can this be solved? There is a theory that could stimulate some of these areas; this is given by Bruce Scheier;
" Personal information protection is an economic problem, not a security problem. And the problem can be easily explained: The organizations we trust to protect our personal information do not suffer when information gets exposed. On the other hand, individuals who suffer when personal information is exposed don't have the capability to protect that information."[9]
Schneier divides this theory in three major problems that have to be solved, two economic and one technical. The two economic problems deal with the following. Organization do not suffer the consequences, legal or financial, when they lose personal sensitive information. As an example Schneier uses the credit card companies. In the past these credit card companies could held the consumer accountable for fraud, up to a certain amount, like $50. Due to this the credit card companies did not spend much money in reducing this problem, until they where forced

9 http://www.schneier.com/blog/archives/2007/05/does_secrecy_he.html accessed May 2007.

by the U.S. Congress. Since then these credit card companies invented all kinds of security measures that reduced fraud. As Schneier concludes: make the party in the best position responsible for the risk, this will enable innovation. If it is in a companies financial best interest to protect people their personal information, they will do it.
Due to the new threat or the bigger threat (if it already existed) companies will try to find new ways to minimize this risk. Within the scope of risk management companies will develop new strategies to deal with this new risk. One of the most embraced theories of risk management, which is also used as exam material for CISSP, is the '4T' theory of Dorfman. According to S. Dorfman companies can do the following four things in dealing with their risks:
"Once risks have been identified and assessed, all techniques to manage the risk fall into one or more of these four major categories: (Dorfman, 1997) (remember as 4 T's):

- *Tolerate (aka retention)*
- *Treat (aka mitigation)*
- *Terminate (aka elimination)*
- *Transfer (aka buying insurance)."*[10]

If we assume that companies will get more responsible for personal sensitive information in a financial and legal way, companies can not longer tolerate this risk as they are doing now. So they will do their utmost to either treat, terminate or transfer the risk. However it is well known that any kind of security will be broken within a certain amount of time, so it is reasonable to assume that terminating this risk is not an option. This leaves companies with two options treating or transferring the risk. Firstly, in the context of transferring risks perhaps a new kind of company or businesses unit can solve this problem. A Trust broker. Such a company will get paid to manage all personal sensitive information of one or several companies, but will take the blame if something goes wrong with this data, e.g. Stolen, leakage, corrupted, et cetera. Furthermore it can perform some functions that are not yet properly handled on the internet, like giving digital trust. Secondly, treating this risk will require several technical and legislative solutions. This will include technical solutions, like; ways to alter the authentication process so that no personal sensitive information is needed and stimulate bi-directional strong authentication. Legal solutions, besides the new laws created by the government, will include things like; try to give better control tools to companies in order to give better insight and decisiveness within the matters of securing and storing personal sensitive information. These subjects will be discussed in more detail further below. Before establishing the functions of a Trust broker and how they will be performed, the following important question has to answered; Why will people and companies entrust their personal sensitive information to a new kind and possibly unknown company? Proceeding from the suggestion that the risk is transferred to a Trust broker and not a new businesses unit. Nevertheless, new company or businesses unit the question remains, why should people trust it?
A good example of trust problem that could arise, is given by Kim Cameron. The example is Microsoft Passport, which was the first to promote an internet wide authentication unification, but as Microsoft and inventor Kim Cameron admitted this was a failure.

10 Dorfman, Mark S. (1997). Introduction to Risk Management and Insurance (6th ed.). Prentice Hall. ISBN 0137521065

"In Passport's case — and it wasn't the only one that failed, by the way — merchants would say, what is Microsoft doing between me and my customer? And customers would say why is Microsoft involved in my relationship with this online store?"[11]

The main reason for this was that people didn't want Microsoft between every transaction they make with another company. After this Cameron had learned a lesson and created a blog that started a broad discussion about identity, this ultimately produced the "Laws of identity".[12] These laws, in combination with all the people that were involved and inspired by this, came up with the idea of an identity meta-system, "Laws of identity". The most important difference with MS Passport is that the third party will not know what all their users will do, thus it will not know every thing about a person. So it is important that a company will not know everything its users does. Another example how people can trust companies is given by IT compliance.

Since the accounting scandals within big corporations, such as Enron and Worldcom, the U.S. Governement established an Act that would restore the public trust in accounting and reporting practices by increasing legislation in a wide range of areas. This Act is called the Sarbanes-Oxley Act, also known as SOX or Sarbox. One of the areas that is covers is ICT, this section places the responsibility of businesses operations and reporting with the corresponding people. To accomplish this SOX uses several control frameworks like COSO and COBIT. With this amount of internal control and the still increasing legal obligations, fraud and carelessness with personal sensitive information will certainly decrease. In conclusion, why people should entrust a new company or business unit is because of several grounded reasons, like financial and legislative:

- A company will not become all powerful by knowing everything about you and with who you deal. This is possible because of its architecture, as explained in the identity meta-system
- Such a company will get paid to do a good job, where good means handling personal sensitive information with care and giving their utmost to protect it. If they don't do this people will not use their services anymore and it will probably be end of business
- If companies are compliant with laws and acts such as SOX, people can presume that the company will take great care of their personal sensitive information. Whereas if they fail, they will pay the price, unfortunately you as consumer are still the one in discomfort

Entities

So now that we have established that people can trust these sort of companies, because of certain financial and legislative reasons, we can ask the next logical question; How can a Trust broker determine how to trust a company? Or to rephrase it, does the way of trusting a person differ from the way that you will trust a company? This depends on the perspective that you use. At the abstract level a person, a company or a device are just the same entities but with different attributes, nevertheless still an entity. By seeing these three characters as entities with different attributes the process of

11 http://www.theglobeandmail.com/servlet/story/RTGAM.20070316.wqandakimcameron0319/BNStory/PersonalTech/home accessed June 2007

12 http://www.identityblog.com/stories/2004/12/09/thelaws.html accessed May 2007

determining trust doesn't change. You still want to know what their identity is, what they do and what their reputation is.
In conclusion, presently we have established what the main function of a Trust broker will be, why it could exist and why entities can trust the Trust broker. In the next chapter the functions of a Trust broker will be determined.

What functions should a Trust broker perform?
With the flaws in digital trust established, and four issues to solve it determined, the foundation for creating the Trust broker is made. These four issues are:

1. What is someone's identity?
2. What do you know about these identities, what are their skills, and how reliable are they?
3. How can you verify and update the information required in issue 2?
4. How can you control and manage the relationship with other parties, in particular legal control?

Which issues should be addressed by the Trust broker, within the context of a Jericho Forum Network? Firstly, identification of an entity. This will be the foremost function of the Trust broker, knowing which entity is communicating with it and assuring a web service or a application that it is really that entity. Secondly, what a Trust broker knows about an identity, skills and reliability. This is difficult; it depends on how a Trust broker gets this information. If an identity gives this information about itself it is not very trusted, but if it is given by someone or something else, it is more trusted. This means that there will be a separation in kind of personal information, self asserted or given by a trusted authority. Which level of trust that is required depends on the transaction or relationship that is about to be performed or used? The third point is a bit two folded, checking and verifying information is a function that is absolutely performed by the Trust broker. However updating this information automatically is not necessarily the task of the Trust broker. It certainly will monitor and collect information about reliability and skills continuously. Although, in order to give the most objective information, the Trust broker can not just update this information in cross reference with similar services. It will always have to check and verify its own information with similar services and data. And the fourth point is legislative control. This is not something that a company or a Trust broker can take care of, it must be done by a government with laws like the Sarbanes-Oxley Act. Nevertheless a Trust broker can be enabled to perform certain legislative duties by combining this digital service with 'real world' services like creating contracts. Some form of a contractual framework can assist the job of the Trust broker on things where the law is not ready yet.

Function	Requirement	Note
Identification	Must	The Trust broker has to know the identity, it can do this by delegating this service to existing network functions. However since the Trust broker is more web oriented it will be better to created a separated service for identification within the Trust broker.
Additional information about the identity, like skills and reliability	Must	Information will be divided in two categories; self-asserted and given by an authority. This will contain information like reputation and past behaviour.
Verifying and updating information about an identity	Must/ could	Verifying must be done by the Trust broker. Updating could be done by a Trust broker. Nevertheless how it will perform these functions depends on the risk. ● With a high risk verifying information will be done by checking other sources, preferably from official authorities. ● With a low(er) risk, verifying information can be done from its own sources. If updating occurs it will only do this with the information from the official authorities.
Legislative control	Must	Although the law is not fully adapted to computer crime, legal support can be implemented by means of contracts.

How can ICT processes perform these functions?

1. The technical process for identification is done with authentication. Within our research group this process is described by Evgeny Barannikov in his thesis Authentication and Accounting. The central process of authentication is that an entity shows or proves to an authority that it is the same entity as before. Technologies that should be used must be compatible with each other to increase usability. Another important point is that authentication and identification can be separated for the Trust broker. Maybe the Trust broker only want to know the identity of an entity and leave the authentication to a specific application or system that this identity wants to use.

2. How a Trust broker learns about its entities can be done by classical registration forms (self-asserted) or by cooperating with other services that will provide the necessary claims, credentials or

attributes about an entity. For self-asserted information reputation systems can be used to increase the trustworthiness of the credentials, e.g. the Ebay, Jyte and slashdot reputation-system. For claims and more trusted information references from government, financial agencies and other companies can be used e.g. Experian.

3. Verifying information at the Trust broker is done by searching the own database or by means of cooperation querying the database of trusted authorities or other Trust brokers. Technologies that support this cooperation in a secure manner are XDI (explained in chapter 9) and an idea of Wouter Teepe in his thesis[13]. In this thesis he explains that privacy and security can co-exits because of some cryptographic functions that can be used in combination with databases. The most important concept that Teepe has used is a pseudonym system. By doing this attributes of entities can be verified without breaking the privacy of the entity. An almost similar idea is used in the IBM identity-mixer[14].

4. Legislative controls with digital contracts are not yet supported. They can be made digitally but have to be signed on paper. It is probable that in the near future digital signatures[15] will become acknowledged by the law enforcement and this will open up new ways to create contracts and control mechanisms for companies. Until that time other means to accomplish legislative control must be found. A way to achieve this is by making a contractual framework, where companies or partners can easily create and monitor these contracts. Technologies that can be used to create such a framework are ws-agreement and link-contracts (as a part of the XDI protocol).

The ICT functions and technical solutions that are needed to perform these processes are described in more detail in the following chapters.

13 http://www.teepe.com/phdthesis/ accessed March 2007

14 http://www.zurich.ibm.com/security/idemix/ accessed April 2007

15 In cryptography, a digital signature or digital signature scheme is a type of asymmetric cryptography used to simulate the security properties of a signature in digital, rather than written, form.

8. What is the potential role of the Trust broker?

Till now the Trust broker is mentioned pretty often, but the global role of the Trust broker within a network is never discussed. This will be done in this chapter.

Potential role of the Trust broker

Essentially the Trust broker must become a central gateway for users to access data or services that are provided by a company.

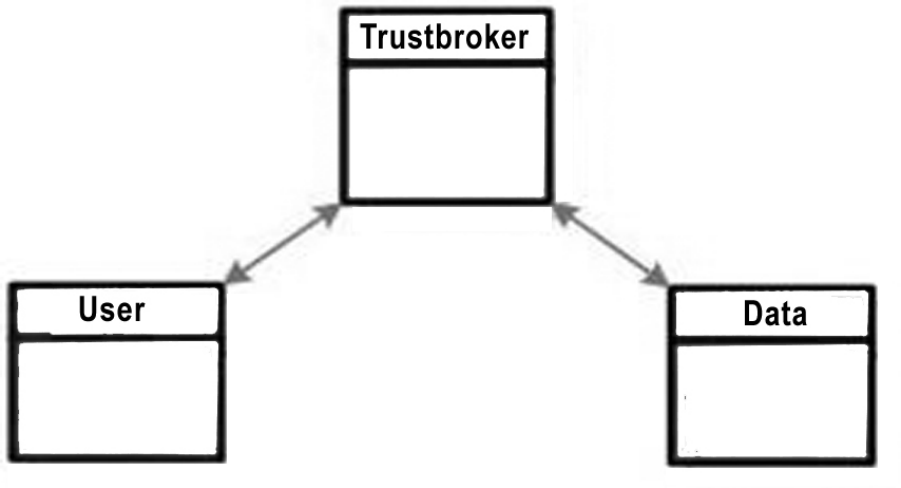

Figure 11: Trust broker architecture within a de-perimeterized environment

In order to do this the Trust broker must be able to provide all processes to create a good and secure connection between the user and the company. This is a enormous task to fulfill, but when implemented correctly the Trust broker should tackle the Jericho Forum Commandment number 6 and number 7. These commandments say, "*all people, processes, technology must have declared and transparent levels of trust for any transaction to take place"*. And, *"mutual trust assurance levels must be determinable"*.

It complies with these commandments owing to the following reasons:

- Trust is applicable to all entities
- By means of contracts, trustworthiness behaviour for establishing transactions is ensured
- Mutual trust assurance levels can determined with the combination of a legal framework and the different Trust broker models.

However, if the Trust broker is implemented as the main gateway that controls everything it violates Jericho Forum Commandment number 10, "*data privacy (and security of any asset of sufficiently high value) requires a segregation of duties/ privileges."* The Trust broker as proposed above is too powerful and shall create a top in the chain of trust. So in order to comply with Jericho Forum Commandment number 10 segregation of duties must be implemented. Segregation of duties is a way to make it more difficult to perform deliberated fraud, because in order to complete a transaction the involvement of two or more parties is needed.

How can the segregation of duties be implemented within the Trust broker?
In order to implement it, the Trust broker must first be sliced into several basic processes, so it can not control more then two steps of an transaction. For example, authentication and authorization will be done by different processes. Frequently segregation of duties is already implemented within the corporate networks, in order to be compliant with the different laws like SOX. It therefore will be reasonable to still use the same network infrastructure and only add one specific element, the Trust broker element. Since a Trust brokers main purpose is to deal with all the external transactions, and most networks today are already tuned to deal with the internal transactions, it should be easy to add the Trust broker to the corporate network. It will have to be added in such a manner that it can cooperate but can not control every process. To accomplish this a framework has to be created that can operate with any local process and will forward its requests to the external service. When structured this way the Trust broker will get a universal appearances to the outside. By creating the same look and feel at any company, the Trust broker will comply with Jericho Forum Commandment number 2. It will be simple, scalable and easy to manage. The advantage of this is framework is that the Trust broker doesn't control everything, but it works together with all the other servers or applications present within the corporate network. Distinctions between the functions that are dealt with by the framework and by the Trust broker itself are determined below. Authentication servers already exist in every network environment. Processes that the Trust broker can handle are sharing this information with partners to create a federated identity. In addition, it also can perform a entirely different authentication server, one that is more dedicated towards internet services, like the user-centric approach. Reputation servers can be separated from the Trust broker, because it is a dedicated system that is constantly monitoring and collecting potentially sensitive data about the entities. The same goes for behavioural systems. To fulfill the Trust broker function these two processes are certainly needed, but the performance can be done by the Trust broker framework. Legal control is very important and should certainly be done by the Trust broker. But as mentioned earlier, due to the lack of support by the law this can not be done in a digital way. To use legal control mechanisms between entities it is most important to created contracts, a contractual framework has to be established. This can be done digitally, with digital signatures or more official by hand, this depends on the trust model that is being used. When contracts are signed with digital signatures, a very important aspect is given by Rafal Lukawiecki. Lukawiecki calls it Trusted Time Stamps. This service will stamp any digitally signed document, so that the date of the stamped document can always be trusted. Even when your digital signature is stolen, copied or just misused the document is still legitimate, because the time stamp can prove a document was signed before the signature was malicious. Another important aspect of contracts is the monitoring of the companies own obligations and if the obligations of the other party are fulfilled. The other functions will be performed by all the other servers/modules that already existed within the network, such as authorization, key or certificate management, auditing, etc.

The Trust broker framework

As mentioned above, to comply with the Jericho Forum Commandments it is necessary to delegate important functions. To accomplish this I suggested a Trust broker framework. This framework will consist of several processes or modules that can co-operate in order to fulfill the Trust broker function. The control that the Trust broker will have over these processes shall be specified. It will be ensured the Trust broker can not change or influence the operation in any particular process to its own benefit.

How should the Trust broker framework operate?

This framework will work just like the ws-security protocol. This protocol is primarily build upon meta-data system were attributes can be simply exchanged between different kinds of protocols. This is made possible by using formats like the extended markup language (XML). In this manner the Trust broker framework will be interoperable with different kinds of technologies and protocols, even with technologies that do not yet exist. This quality lets the Trust broker framework comply with the Jericho Forum Commandment number 4, *"devices and applications must communicate using open, secure protocols"*. When this interoperable framework is created modules can be added to expand the functions a Trust broker can perform.

What are the benefits of these different modules?

Such a framework has several advantages, because of its modular building blocks:

1. you can simply change one module with a new or better one
2. it should be possible to let several modules with the same function load balance each other,
3. with all functions operating in different modules the Trust broker won't become a single point of failure (SPOF). If the Trust broker fails it will only disable the ability to communicate and facilitate services with the outside
4. modules do nor necessarily have to be in the same (geologic) location This will enhance right shoring and off shoring capabilities
5. a framework with the underlying meta and object-oriented architecture can operate for a long time, because modules can be simply updated or expanded
6. the modules can be created from the services that are already present on the network, being practical and cost efficient. This supports the JFC number 1
7. because each module is its own 'master' it will has its own security policies and logs, thus making it easier for auditing and compliance checks. It also complies with the JFC number 5
8. communication between modules is largely dealt with by web-protocols. This way there will be no real distinction between your network and the internet. Plus you can choose from many proven security solutions for web-protocols

When the Trust broker framework is implemented, how secure will it be?
Possible vulnerabilities will be the same as the existing threats on the internet. Most security threats of the Trust broker framework will be based around the connection between the different modules. The modules itself should be rather secure, because each module will have installed its own security measurements as described by Leon Teheux in his book 'Jericho in depth… Authorization & Endpoint Security, Capgemini 2008'.
To give two examples of security vulnerabilities concerning the communication:

1. man in the middle attack between modules within the framework, especially when modules are in different (geologic) locations
2. hacks are security flaws within security protocols. When this occurs the possibility that personal sensitive data can leak to the internet increases

To enhance the security of the framework all kinds of encryption standards can be applied in combination with the newest security protocols. To prevent man-in-the-middle attacks all modules within the framework will have to authenticate to each other, bi-directional or mutual authentication. Ways on how to do this, from a encryption point of view, are explained by Alina Stan in her thesis 'Jericho Forum Project: End-to-end encryption, Capgemini 2007'. Hacks and security flaws will always remain a problem, but when using open protocols the response time of the community will be very high in most cases. This means that potential security risks are always short lived.

Legal framework

In this chapter the different models for creating a physical Circle of Trust is described through the use of a contractual framework as suggested by the Liberty Alliance; "*Liberty recommends that the parties implementing a federated identity or a identity-based network need to establish a contractual framework for a legally binding Circle of Trust that obligates the parties to abide by certain agreed upon obligations, rules, and remedies that will govern their relationship.*"[16] This is very useful especially from the perspective of risk-assessment. This fulfills the need that digital contracts and signatures are lacking, namely support of the law. In this contractual framework a number of topics are dealt with, such as Roles, Rights and Obligations, Confidentiality, Enforcement & Remedies, Entrance and Exit of Members, et cetera. According to Liberty a contractual framework will lead to a robust and trust worthier Circle of Trust (CoT) between the participants. In order to implement this framework amongst the parties a organizational model should be chosen. Liberty has given three organizational frameworks to do this:

- **a.** collaborative model
- **b.** consortium model
- **c.** centralized model

Each of these models has its own specific rules, regulations and policies. Below some of these characteristics shall be shortly explained.

16 http://www.projectliberty.org/liberty/content/download/2962/19808/file/Liberty%20Legal%20Frameworks.pdf accessed April 2007

A. Collaborative Model

"As depicted in the diagram below, a group of Founders forms an entity that establishes the rules for the operation and governance of the CoT, and then also undertakes the day-to-day governance of the CoT. This approach is perhaps the most complex, but arguably provides the most flexibility for a large CoT with many Founders and fluctuating membership – and once the initial work has been done to establish the Governing Entity, this model provides a single consistent entity with which to contract."

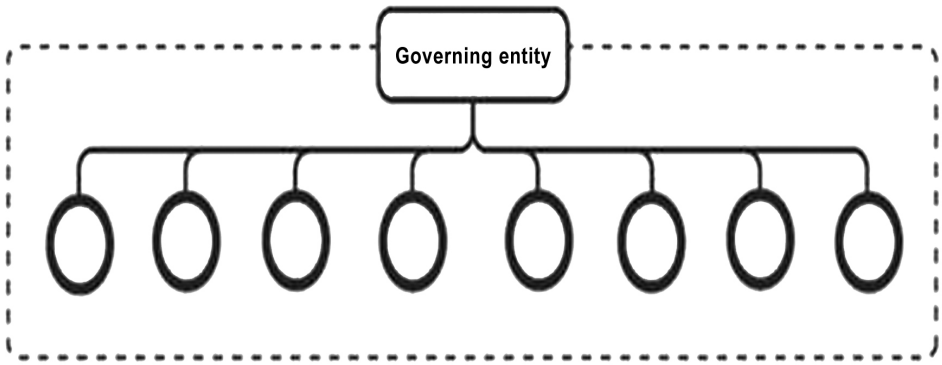

Figure 12: Collaborative model (adopted from the Liberty Alliance Legal Framework)

B. Consortium Model

"A small number of Founders forms a consortium via a multi-party contract that sets the rules and governance for the CoT. This approach offers more direct control by each of the Founders. However, this model is not recommend where the membership is in flux, as the ongoing entrance or exit of members of the CoT is likely to be cumbersome and require amendment to the consortium agreement. Following is a diagram of this approach."

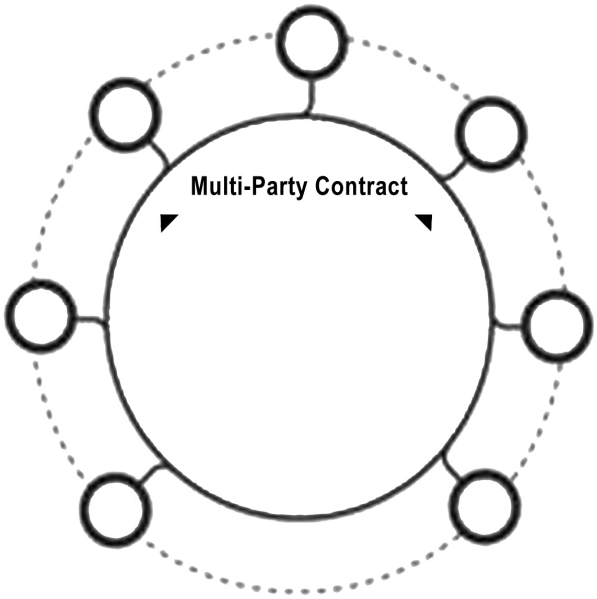

Figure 13: Consortium model (adopted from the Liberty Alliance Legal Framework)

C. Centralized Model

"A single Founder sets the rules and governance for the CoT, and contracts individually with each other Member. This approach provides the Founder with a significant amount of control, and significantly less control to the other Members. As the diagram below implies, the Founder may use this model to establish two-party relationships, n-party relationships, and relationships in which it (the Founder) acts as an intermediary between other entities (partners, suppliers, customers and so on)."[17]

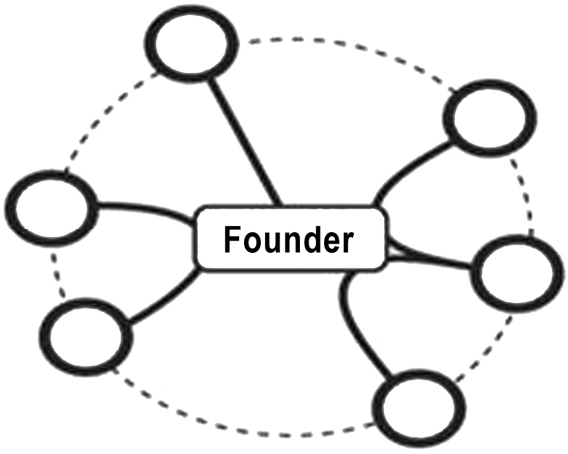

Figure 14: Centralized model (adopted from the Liberty Alliance Legal Framework)

The table below will summarize the different models, including their advantages and disadvantages.

Circle of Trust models	**Advantages**	**Disadvantages**
Collaborative model	Appropriate for large CoT, where members are in flux.	Members must cover the expenses of the new entity.
	No member has to govern and enforce the CoT.	Not appropriate for establishing simple contractual mechanisms.
	Possibility in shifting the liability towards the new governing entity.	And less enforceability towards each member.
Consortium model	Appropriate for a small and steady CoT.	Not one entity has control over the CoT.
	Each member has direct control over the CoT. Increasing contractual commitment and enforceability	Has no liability shield that a governing entity provides.
Centralized model	The sole founder has full control over the CoT.	Can not share the responsibility and the cost among the members.
	Membership can vary easily, due to low entry requirements.	Has no liability shield that a governing entity provides.

17 http://www.projectliberty.org/liberty/content/download/2962/19808/file/Liberty%20Legal%20Frameworks.pdf accessed April 2007

As shown in these models can give a single founder or a combination of multiple founders the legislative control for collaboration and federation. Within these Circle of Trust the Trust broker can operate at its full potential.

Trust broker models

Previously I have presented the framework proposed by Liberty containing the models for the creation of a physical Circle of Trust (CoT). Further, I will describe the Trust broker models that can operate within these CoT models.

Central Trust broker

As the word 'central' implies there shall be only one Trust broker active within a CoT. All parties wanting to establish a transaction or want to use a service that is facilitated by the Trust broker will communicate directly with the Central Trust broker. Giving it the topology of a star network.

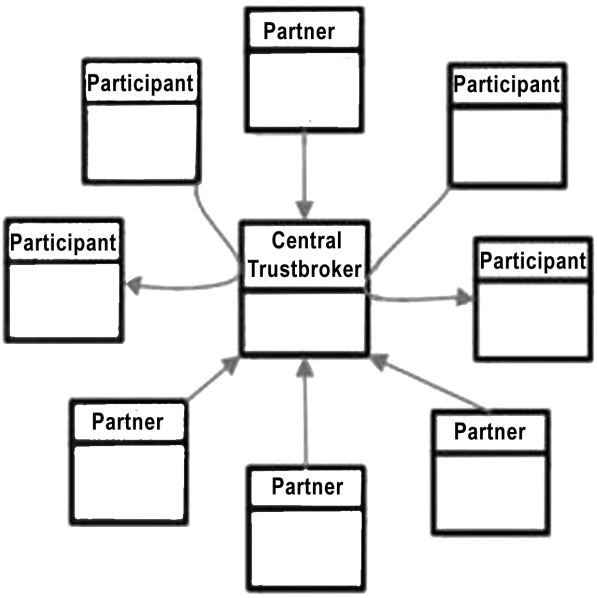

Figure 15: Central Trust broker star network model

Activities that the central Trust broker will handle are:

- managing all the trust relationships between clients and between clients and server
- enforces global security measures and policies to all parties it deals with
- enforces its own security measures and policies to all its hosts
- manages the federation of identities
- keeps records of the reputation and behaviour of the other parties
- monitors all the contract obligations between parties

The Trust broker is able to perform some of these activities based on the information it gets from the participants. This is called a pull-model, the information request originates with the central server. The advantage of this model resides in the fact the management of all the activities performed by the Trust broker is simple, straightforward, and convenient in the case of intermediary functions, and allows for dynamic structures within the model. These advantages derive from the fact that the central Trust broker

will be the only one, within the context of establishing transactions, to enforce security measures and policies. The main disadvantages of this model are derived from the central character of the Trust broker, namely it can become a single point of failure and can be subject of fraud attacks. Fraud attacks are made possible due to the fact it will be the only server delivering all the necessary information. Even with segregation of duties implemented this will remain a problem.

Server / client side Trust broker

The model consists of a server Trust broker and several client Trust brokers. The topology used between the server and clients is resemblant to the Central Trust broker topology, a star network. But this model divides and expands it activities by using a server and a client.

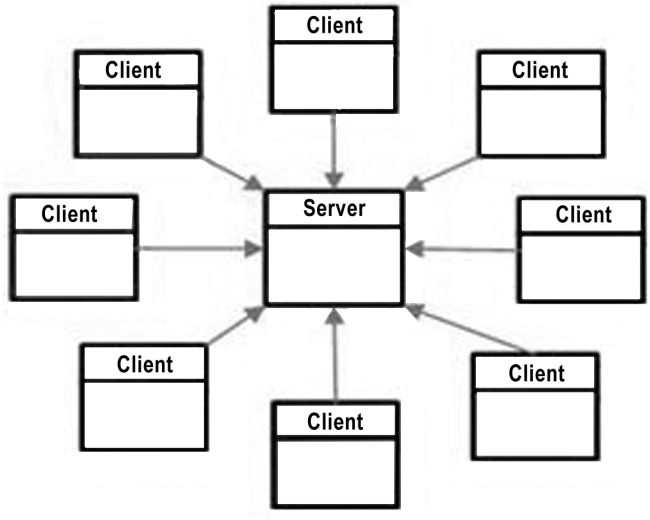

Figure 16: Server/client side Trust broker star network model

Activities that are handled by the server are:

- managing the federation of identities
- keep records of the reputation and behaviour of the transactions between clients and server
- keeps copies of all the obligations that there are between its clients
- will enforce global security measures and policies on to the clients
- can provide a unique role with providing and storing PKI keys and certificates

Activities that are dealt with by the clients are:

- keep records of the reputation and behaviour of the transactions between clients
- keep records of the obligations is has with all of its clients
- will enforce global security measures and policies to all the transactions it makes with other clients
- will enforce its own security measures and policies to all its own hosts

Advantage of this model is that if information is required by one of the Trust brokers it can be updated real-time. This is made possible by the continuous communication

between the server and its clients. This model is called a push & pull model, because it does not matter where the request for the transmission of information originated. A side effect of this server/client model is that information is more trustworthy. This because the information is easily accessible and available, plus there are more sources with similar information. Possible disadvantages are that it can be rigid, because a new party will first have to redesign their network in order to incorporate the client Trust broker.

Peer-2-peer Trust broker

This model consists of a community of Trust brokers where each peer will perform the same activities. The network topology that is created by this community can be compared with the internet, a fully connected model.

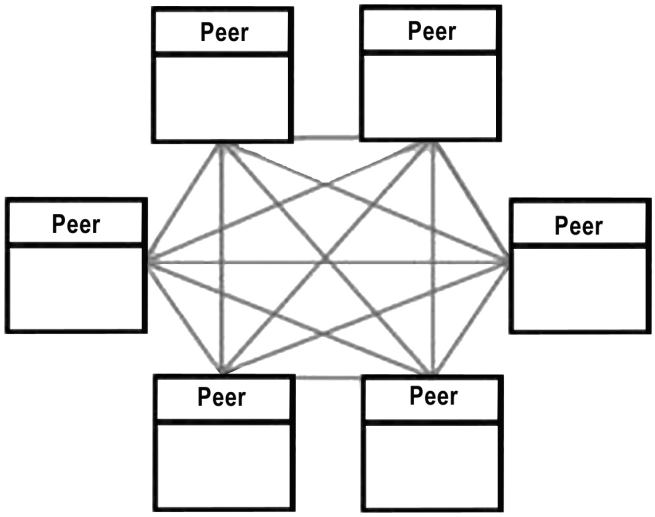

Fig. 17: The peer-2-peer Trust broker full connected network model

Activities that each peer will perform are:

- managing all the trust relationships between peers in deals with
- enforces global security measures and policies to all parties it deals with
- enforces its own security measures and policies to all its hosts
- keeps records of the reputation and behaviour of the all the parties it deals with
- monitors all the contract obligations between parties it has an agreement with

However, as a community the peers together can deliver specific functions that are not performed by a single peer. Functions like:

- managing the federation of identities
- keeping copies of all the obligations that there are between peers
- enforcing global security measures and policies on to its community of peers
- can provide a unique role with providing and storing PKI keys and certificates by dividing the information over the peers

Advantages of the peer-2-peer Trust broker are that there is no obvious 'leader' or server and this reduces the likelihood that it can become a single point of failure. In addition to this, a fully connected network architecture and many similar peers performing the same functions support the prospect of load balancing. Load balancing can offer an increase in resource utilization and computing time by spreading its workload across several peers. Disadvantages can be that this peer-2-peer Trust broker is very difficult to manage. This difficulty will arise due to the distribute approach in performing functions by the community of peers. To improve this it a hybrid model can be chosen. In this hybrid model specific designated peers are will perform and manage the functions as mentioned above.

Trust broker models	Advantages	Disadvantages
Central Trust broker	Relative simple and straightforward management.	Can become a single point of failure.
	Able to perform intermediary functions.	More likely to be subject of fraud attacks.
	Allows for dynamic structures within the model.	
Server/client Trust broker	Continuous communication between the server and its clients, creating a push & pull model.	Have to redesign your network in order to incorporate a client Trust broker.
	There are more information sources that are easily accessible and available, creating more trustworthy information.	
Peer-2-peer Trust broker	No obvious server, reducing risk of single point of failure.	P2P structured network is difficult to manage.
	P2p structure and a fully connected network creates opportunities to perform additional functionalities.	

The integration of the Trust broker models within the different Circle of Trust models

Previously, I presented the different models for creating a physical Circle of Trust, and the Trust broker models of interest for this thesis. Further on, I will analyze the possibilities of using the Trust broker models within the Legal framework models, or the so named, Circle of Trust (CoT) models. The combination of these two models will enable the Trust broker to use enforcement mechanisms on its clients by the use of contracts. By fulfilling this requirement it is demonstrated that all functions of a Trust broker can be performed. For the first two CoT models, Collaborative and Consortium model, two different Trust broker models can be applied. This can be a peer-2-peer or a

server/client side Trust broker . It will depend on the nature of the data or services for which the CoT was created to chose between these two Trust broker models. If the services and data, that are delivered by the different founders, are very similar a peer-2-peer Trust broker will have more advantages. But when these services differ respectably it will be wise to chose a server/client side Trust broker, because the more hierarchal approach it will deliver order between the various services.
When given the nature of the collaborative model it will be most likely to use the server/client model, because of two reasons:

- the governing entity will create a hierarchal structure, just like a server/client model
- the governing entity has lesser enforcing control over its members. This can be compared to the way the server enforces its policies upon its clients, but every client can create their own policies to enforce upon its hosts

In case of the consortium model the peer-2-peer Trust broker will be the most suitable, because of the following corresponding properties between the two model:

- a consortium model does not have one single point of control
- each member has a reasonable amount of enforcing capabilities over other members

In order to operate the above two models share their control mechanisms, the Centralized model does not share this capability. Consequently a Trust broker model is needed that that is able to give full control, this is done by the Central Trust broker. Due to the facts that these two models have full control and can easily change its members, it creates a unique possibility to become an intermediary. This function can deliver interesting business drivers and services, considering the fact that it will accomplish to create trust between two distinct parties, which enables them to perform business. In conclusion, the combination of the Trust broker models with the Circle of Trust model will give the Trust broker the enforcement mechanisms it required. By fulfilling this need it is proven that all functions of a Trust broker can be performed.

In which identity models can a Trust broker function?

Previous chapters established that identity plays a central role within the functioning of a Trust broker, it is therefore important to know which identity models can best be adopted. In this chapter I shall describe the three identity models within the context of the Trust broker. The three models are a central, federated and a user-centric model. These models are described in more detail by Evgeny Barannikov in his thesis ‘Jericho Forum Project: Authentication and accounting, Capgemini 2007'.

The central model

A central model only serves one domain. Within this domain there is only one directory where all the entities are stored. Managing only one directory should make identity management easy for administrators, but it makes the creation of trust relations between different domains very hard to accomplish, and even harder to manage. The reason why it is hard to accomplish is that within a central model it is difficult to communicate with other domains, it therefore prevents to the establishment of trust between domains. Unfortunately this model is still used in lots of companies nowadays. This is because the model is simple and well known, but it has its restrictions in communicating beyond the perimeter. Due to new business drivers and new technology

even smaller companies can and are changing to other models. The Trust broker can not reach its full potential in a central model. However, it can simplify managing trust relations but due to the lack of interoperability between domains it only provide the service to some extent, such as sharing data and services across different domains. So the central model is, as said in the Jericho Forum business case, a restricted communication model. This model is not ideal for the Trust broker, as the Trust broker depends on communication with external parties.

The federated model

The federated model main goal is to share identities with different partners between different security domains in order to reduce costs and increase usability. To simplify federation it must become possible to use open industry standards or open specifications, so all parties can achieve interoperability. This interoperability will enable features such as web-based single sign-on, cross-domain user account provisioning, et cetera. In other words make the system and the network more usable for the users. A big business driver why companies want to adopt a federated identity is because in general they don't care what your username and password is, they only want to be sure it is you. So if this process of being sure that are who you say you are can be shared or distributed across several trustworthy parties it means that the individual cost can be reduced. From the Trust brokers point of view this federated model is a great model to start with, as it envelops its perimeter across multiple companies while each company is still secure. The Trust broker can easily facilitate the process of managing the identities between the different companies and can serve as a uniform gateway for sharing data and services between these partners. In conclusion, with a federated identity model the usability for the users increases whilst the total cost of ownership decreases. As such it is a great model to implement a Trust broker.

The user-centric model

As the the word user-centric implies this model focusses its attention on the user, enabling the user to get full control over his identity. To elaborate on this, the user-centric model attempts to imitate the real world. In the real world a person can choose which identity it shows when he is asked to identify himself in a store. For example, think of all the different cards you have in your wallet. The user can choose between his passport, drivers licence, student card, etc. All these cards will say something specific that identifies a certain aspect of your personality. In a user-centric model, this information is called a claim. A user-centric model is based upon a claim-based system. So in comparison to the central model where someone is identified by a directory entry, now a person is identified through the claims it can show about itself. By identifying users based on the presented claims instead of checking a directory, thus user-centric model becomes the opposite of a central model, namely a decentralized model. Since it allows the storage of identity information outside the area of control, the decentralized model is able to support the concept of de-perimeterization.

The decentralized model is very convenient for the Trust broker, since the Trust broker will have little problems with collecting data about the user. Furthermore it can facilitate its services around the world due to the architecture of a claims-based system. This architecture enables it to send claims easily to any service around the world through the use of protocols like eXtensible Markup Language (XML). This user-centric model is not

only good for users it also good for business, considering it stimulates businesses connectivity with partners. In addition it provides a way to easily split business processes across several partners, which will probably lead to a reduction in cost. Thus a user-centric model has several advantages, it being good for business and users, and it perfectly matches with the de-perimeterization concept, thus making it the best identity model to implement within a Trust broker. However, to use this model the claims-based system must be supported by all partners, according to Dick Hardt from Sxip Identity this will be supported in the very near future.

Conclusion

In conclusion, the identity model that is best suitable for a de-perimeterized environment is the user-centric model. However, the claims-based system, which is the foundation of the user-centric model, is not yet supported. Due to this reason the federated model is presently the best suitable identity model to apply within the Trust broker and a de-perimeterized network.

9. Relevant technology development

Previously we established how the Trust broker would function. To continue I shall search for relevant innovative projects present on the market that are comparative with the functions of the Trust broker. I shall divide this in three research areas, authentication, reputation and behavioral analysis.

Authentication

As established in previous chapters, authentication plays an important role within the Trust broker. Further on I will explain shortly what authentication is and which technologies are currently (may 2007) on the market or under development. Authentication is the process that verifies a digital identity in order to give the sender of this digital identity access to a resource at some authority. This identity can be a real live person, but it can also be a computer or an application. For the authority it is most important to know for certain that a digital identity is the same as before. In order to determine this the digital identity must show some prove that it is the same entity as before. Which information the entity has to show depends on the level of authentication, for example low security levels will suffice with only one factor of authentication, such as only something you know, better known as username and password. But if an entity wants to get access to something with a high security level some type of strong authentication is needed, such as what you know, what you have and perhaps what you are. This can be done with a username, a device that gives a password and perhaps a fingerprint or iris scanner. An example of software that handles all these entities is a Identity Management (IdM) system. IdM is much more then just a authentication system, it handles the hole identity life-cycle. This life-cycle exists of creation, description and deletion of a identity. The problem with todays authentication process on internet is that there are too many different identity silo's where attributes of an identity are stored. In each case having a different username, different password, et cetera. This is getting very difficult for people to remember. Another point of concern is that the strength of the passwords that people use is decreasing[18]. There are some initiatives on the market that try to tackle this problem. Below I will discus some of the most favorable or just well known.

Microsoft Cardspace

Microsoft Cardspace is the most well known initiative present. This approach is one of the first commercial products that uses the architecture of "The Identity Metasystem".[19] This architecture is invented by Kim Cameron, his vision was to develop an extra layer on the internet that handles all identities. To accomplish this an interoperable architecture had to be created that could handle multiple identities from different kinds of technologies and providers. By implementing this users can get back in control of their identity and organization can keep using their existing technologies, but will still be able to maintain a level of interoperability with others technologies. The way that Microsoft tries to accomplish it is by making an 'identity selector' based on how people use a wallet with business cards. Each card represents an identity, but does not contain

18 http://www.security.nl/article/14423/1/Analyse_van_20.000_gephishte_MySpace_wachtwoorden.html accessed May 2007

19 http://www.identityblog.com/?page_id=355 accessed February 2007

the actual identifying information. This information is given by an 'identity provider' or can be self-asserted. The actual data that is sent is a signed and encrypted security token. This token is first sent to the user himself so it can check the data that is about to get sent, after his approval this token is sent to the relying party in order to get authenticated. The main advantages of this technology is that phising and man-in-the-middle attacks become far more difficult, but unfortunately not impossible. MS Cardspace will be shipped with MS Vista, but will not be exclusive to this platform. Because Microsoft understands the problem is deep and no one vendor or technology can solve it alone they made WS-* is an open standard at the OASIS standards organization. Microsoft and IBM have made a royalty-free license commitment for WS-* that is consistent with the OASIS IPR policy. Luckily this complies with the JFC number 4, it demands that all devices and applications must use open and secure protocols. Because of this royalty-free license there are a few open-source projects that are implementing this architecture and protocols in order to create multi platform computability.

Bandit

This open-source project is supported by Novell. Its goal is create a open and standard identity infrastructure. To create this infrastructure it uses many different open-source projects like Higgins, CASA, OpenXDAS, et cetera In the context of authentication I will continue with Higgins.

Higgins

"Higgins is an open source software project that is developing an extensible, platform-independent, identity protocol-independent, software framework to support existing and new applications that give users more convenience, privacy and control over their identity information."[20] The idea that Kim Cameron has with 'the identity metasystem', is being realized by Higgins. As mentioned above they are creating a true platform- and protocol independent framework for a more better and secure identity infrastructure. In order to realize this they are implementing the following techniques, ws-security, openid, saml.

OpenID

OpenID is a decentralized identity management system. The main idea is that you will have multiple identities at multiple silos and that you can combine these silos with your OpenID URI. Openid is getting a lot of positive attention the last few months. Microsoft has implemented it into its own Cardspace, AOL has adopted it, and the number of providers that are hosting Openid keeps on rising. OpenID started as just a single-sign-on solution, now OpenID 2.0 has a true user-centric approach.

EXtensible Resource Identifier (XRI)

XRI is a new scheme protocol for abstract identifiers that is compatible with URI (Uniform Resource Identifier) and IRI (Internationalized Resource Identifier). *"The goal of XRI is to provide a universal format for abstract, structured identifiers that are domain-, location-, application-, and transport-independent, so they can be shared*

20 http://www.eclipse.org/higgins/faq.php accessed April 2007

across any number of domains, directories, and interaction protocols."[21] The main benefit is that XRI can identify any resource, such as organisations, people, machines, applications, digital object, et cetera. Some examples that are possible with XRI are[22]:

- Organizational or personal ID used for multiple purposes (e.g., contact page, IM, email) One XRI address could be used to identify somebody or something by linking it with virtually unlimited resources or communication channels. These resources or channels can be a contact webpage, a blog, a mail address, a telephone number or anything the user wants
- Single sign on a single sign on system like SAML has defined operate across the internet domain. XRI can be very useful to support SAML with its identifier scheme because of its human-friendly form
- Books in multiple libraries With XRI cross-reference it becomes possible tot identify a single book owned by more libraries with different identifier schemes, such as ISBN and Dewey Decimal system
- Auditable and trusted resolution In order to comply with the latest regulatory requirements, such as Sarbanes-Oxley Act, the XRI trusted resolution makes it possible to ensure these companies that they are communicating with and about known parties. And also delivers a way to make a audit trail that can be saved for later review
- Purple numbers (transclusions). These numbers are a method for referring to chunks of content in a web site or to include the content on other pages (transclusion). With XRI these chunks of content are easily identified across multiple sites

Reputation system

As with authentication, here the current developments on the market concerning reputation systems. The main reason why a reputation system must be used is to give a entity specific information about another entity, thereby making it possible to come to a well informed decision about whether or not to build a trust relation with that specific entity. This specific information will consist of certain entity attributes, e.g. criminal record (yes/no), address, passport, et cetera. For organisations this can be a registration at the chamber of commerce, the annual report, et cetera. Besides the attributes there must also be some kind of information about its past behaviour in a specific area, e.g. past transactions or obligations fulfilled or not. How these reputations are created depends on the system that is used, but they all rely on the cooperation and input of users. Sometimes the user must be a part of the circle of trust, e.g. the buyer. A problem with these systems is the user, how reliable is the evaluation of the user? Best practices have shown that the user can be a reliable source, although there are known attacks that undermine these systems. The most well known is the Sybil attack[23]. In this case an attacker creates a lot of accounts under pseudonyms and because of its large numbers it will influence the reputation. For a reputation system to work it must consist of some certain properties. "*To operate at all, reputation systems require three properties at a minimum:*

21 http://en.wikipedia.org/wiki/XRI accessed March
22 http://www.oasis-open.org/committees/xri/faq.php#_Toc121168681 accessed March 2007
23 http://www.cs.rice.edu/Conferences/IPTPS02/101.pdf accessed June 2007

- *Entities are long-lived, so that there is an expectation of future interaction*
- *Feedback about current interactions is captured and distributed. Such information must be visible in the future*
- *Past feedback guides buyer decisions. People must pay attention to reputations*"[24]

The next systems that I will discuss are some well known initiatives or market leader at their own specific field.

eBay feedback system

The most well known and most controversial reputation system today is the one from eBay. This system is more a feedback system because it enables sellers and buyers to leave feedback with regards to the transaction that they have made. This system enables people to build a reputation within the community of eBay. This reputation, if positive, can improve future transactions because people will be more acceptable to person that has proven himself reliable. The eBay feedback system is partially peer-2-peer because the community decides the reputation someone has and other members will trust this opinion. This in principle is the way in which a p2p reputation system works. But in this case it does not fully apply as eBay stores this information locally, so when people trust the opinion of the community they also trust eBay that they have not hacked the system and altered the reputations. Unfortunately some people always want to cheat, so they are finding more and more ways to artificially boost their reputation. One of the most popular ways is shown in a new study out of the University of California at Berkeley's Haas School of Business. According to this study people will sell objects for practically nothing to get a positive feedback in return.[25]

Jyte

Jyte is a simple service to make claims, credibility and contacts to build a reputation. The thing that makes jyte special is that it uses the new authentication technology I described above, OpenID. With this feature it becomes possible to take your claims with you to other services that support OpenID. Because Jyte depends solely on OpenID for authentication it is a good solution to create a online reputation system for social networks (p2p), with the difference that you can use this reputation at other services.

Experian

As the Jericho Forum suggested the credit services that this company is delivering can be the bases of reputation management for the business-two-business (b2b) and business-two-consumer (b2c) market. Its sole purpose is to provide businesses with consumer credit data. Experian now only focuses on certain segments in the market, but this kind of system can be expand to any business segment. The reason that this is important is because there must be a system that is built on reliable facts from trusted companies that will give consumers a specific credential. These companies have more specific information about people then friends will know, so a p2p reputation system can only be feasible till certain levels.

24 http://www.si.umich.edu/~presnick/papers/cacm00/reputations.pdf accessed May 2007
25 http://news.com.com/8301-10784_3-6149491-7.html accessed June 2007

Behaviour management

The last subject to make a trust system work is behavioural management, but not in the traditional sense. This system only has to check the obligations that a entity has agreed to comply with. The line between behavioural and reputation is actually very thin, they both want the same information. The most important difference is that reputation says something about your past behaviour and behavioural management will tell something about your current actions. Within the Trust broker, behavioural analyses must say something about the reliability of an entity to fulfil his obligation to the contract that has been agreed upon. As far as the digital realm allows it, it must scan the agreement/ contract and determine if the other party is obliging to it. In order to do this there must be control over the digital contract and the data or services that are linked to that contract. Although the Trust broker only needs to know if the other entity oblige, it can use the more traditional functions of the behavioural systems to support its analyses. This can vary from network monitoring to behavioural analyses. Furthermore, this information can also be used to update the reputation system.

XDI & Link contracts

XDI (XRI data interchange), is a secure, extensible service for linking, sharing and synchronizing data over the internet through the use of extentisble markup language (XML) and extensible resource identifier (XRI). There main goal is to enable data from any source to be identified, described, linked and synchronized in an active, machine-readable dataweb just as hyperlinks did for content on the web. The other most important function of XDI is 'link contracts'. Link contracts enable the owner to get in control of their shared XDI data. It can do this because it is a two-dimensional XML-document which gives active control to the flow of information by 'push' or 'pull'. This control can be performed on a wide range of governing points, just like real-world contracts.

For example, "*link contracts can govern:*

- *Identification: Who are the parties to the contract and what data does it cover?*
- *Authority: Who controls the data being shared via the contract?*
- *Authentication: How will each party prove its identity to the other?*
- *Authorization: Who has what access rights and privileges to the data?*
- *Privacy and usage control: What uses can be made of the data and by whom?*
- *Synchronization: How and when will the subscriber receive updates to the data?*
- *Termination: What happens when the data sharing relationship is ended?*
- *Recourse: How will any disputes over the contract be resolved?*"[26]

WS-Agreement

"Web Services Agreement Specification (WS-Agreement), a Web Services protocol for establishing agreement between two parties, such as between a service provider and consumer, using an extensible XML language for specifying the nature of the agreement, and agreement templates to facilitate discovery of compatible agreement

26 http://en.wikipedia.org/wiki/Link_contract accessed May 2007

parties. The specification consists of three parts which may be used in a composable manner: a schema for specifying an agreement, a schema for specifying an agreement template, and a set of port types and operations for managing agreement life-cycle, including creation, expiration, and monitoring of agreement states."[27]
Currently the ws-agreement protocol is intended to be used for technical Service Level Agreements. The framework that is created can be used to monitor any agreement, as long as it is supported with the right appliances to manage the guarantee terms.

General technologies

These technologies have no direct function within the Trust broker but can facilitate a huge fundamental groundwork to make the concept work. These technologies or frameworks will deal with security of communications between web-services.

WS-* protocols

A collaboration between Microsoft, IBM and Verisigns, since 2004, has led to some new security protocols, WS-*. The star implies that it is a set of protocols that are modularly built so each developer could use the web service protocols they need. These protocols cover a wide range of domains in which they operate, management, security, portal & presentation, transactions & business processes, transferring, and metadata. The most well known ws-protocol is the ws-security or, since it was officially released from OASIS-OPEN, WSS. WSS specifies how integrity and confidentiality can be enforced in Web Services messaging. WS-policy is a set of specifications that allows the creation of digital policy for intermediaries and end points, and how to associate these policies with services, thus making it possible for web-services to advertise a policy through XML, and specify the policy requirements to the web-services consumers. WS-Trust makes it possible to create, exchange and validate different security tokens by using the security mechanism from WSS. This is also possible within different trust domains. WS-Federation is a specification that builds upon the specifications from wss, ws-trust and ws-policy. WS-Federation specifies a mechanism to allow different security domains to federate by allowing and brokering trust of identities, attributes and authentication between web-services.

Liberty Alliance

Liberty Alliance is an alliance of about 150 companies including some global technology vendor as well as multinationals in different segments. Liberty Alliance was formed in 2001 to develop a industrial standard for security issues like authentication, privacy and online indentity management. Since then it influenced many projects on this subject, but the two main products are ID-WSF (identity based- web service framework) and ID-FF (identity based- federated framework). ID-WSF is a framework that works with some specific open standards and protocols to ensure web-service security. ID-FF is also a framework based on open standards and specifies how to make a secure, multi-vendor federated network. These information technologies are certainly going to influence the future of the internet, nevertheless these are not the only technologies to do so. For example, the underlying technologies for ws-security and ID-WSF are the technologies

27 http://www.gridforum.org/Public_Comment_Docs/Documents/Oct-2005/WS-AgreementSpecificationDraft050920.pdf accessed May 2007

that make these things possible.

SAML 2.0

"SAML defines an XML-based framework for communicating security and identity (e.g., authentication, entitlements, and attribute) information between computing entities. SAML promotes interoperability between disparate security systems, providing the framework for secure e-business transactions across company boundaries. By abstracting away from the particulars of different security infrastructures (e.g., PKI, Kerberos, LDAP, etc), SAML makes possible the dynamic integration necessary in today's constantly changing business environments."[28]

Things that make SAML special are:

- It is platform independent
- It does not depend on any vendor, making it ideal for the Jericho Forum as it is an open protocol with security build in
- Is loosely-coupled meaning it is not necessary to maintain and synchronize user information between directories
- It enhances the online user experience because of its unique single-sign-on abilities

These four main aspects make SAML the perfect protocol or standard for realizing a federated network. Since it has been approved by OASIS in march 2005, it has already been implemented in many organizations around the world. The most known company using this standard is Google. Users of Google services can immediately experience the benefits of SAML by switching from their Google mail to their calendar or Picasa service without repeating the authentication process.

Which technologies will help building the Trust broker framework?

To conclude this chapter of relevant technologies, I shall make a global description to help explain where these technologies can be used. In addition some extra general technologies are introduced that are not specific to this subject or for security in general, but can nevertheless increase the functionality or performance of the Trust broker. I shall start with the physical Trust broker. During the last months virtualization has been a hot topic in the ICT branch, according to Gartner it will be a top priority until 2010[29]. The most promising technique in my opinion are blade servers, especially the ones from Egenera. They have tried to make the equivalent of Storage Area Network(SAN) for computing power, thus creating a Processing Area Network (PAN). This network is being controlled by a PAN-manager, this manager simplifies the management of a network because it is mainly virtual. By doing this in a virtual realm and not physically it reduces or eliminates manual, resource-intensive systems administration tasks. And increases the adeptness of the network, because servers can easily switch from location, operating system or processing power with only a few mouse clicks. An other big advantage is that load-balancing and overcapacity are easily optimized, this can reduce the total cost of ownership while still increase the total processing power. Another benefit that could arise when using this virtual environment is the creation of

28 http://www.xml.com/lpt/a/1525 accessed May 2007

29 http://weblog.infoworld.com/virtualization/archives/2007/05/gartner_says_vi.html accessed May 2007

application or services specific boxes. These specialized boxes can be secured in a very specific way, fully customized to this application only. Each of these virtual boxes could apply a different policy. Furthermore the Trust broker framework, since the framework must be able to co-operate with different modules across the globe I think it will be wise to that the basics will operate on web-technology, such as ws-security, -trust, -privacy and -federated. This will create a flexible and robust solution that will be able to communicate with every kind of protocol, through the use of XML and SOAP. Security is build into ws-security by means of XML encryption, which in my opinion is great because it only shields a part of the message but still shows all the parts that are necessary for the transport of the message. This increases end-to-end security, as it is not necessary to give all nodes between the two communicating sources a key for deciphering. Technologies needed for the applications such as reputation management and behavioural management are; jyte, ebay feedback system, experian, ws-agreement and link-contracts. But these technologies will only form the basics, they will have to be fine tuned in order to co-operate. Furthermore these technologies must be able to complete each other to make a conscientious assessment about an entity. There must be made a link between the information stored by accounting and the information for a reputation- and behavioural-system. With this information a reputation can be based on facts instead of opinions from others, like jyte and eBay do with their system. However such a system can get in trouble with the government because of its privacy violation nature. Like Google now experiences with the EU.[30] The storage of this sensitive information is also an important subject. Cleversafe proposed a Dispersed Storage Grids™, to separate data into 11 packets and separate them over 11 different servers. Of course this manner can only be used if the data is not accessed very often, because of the time delay it has when accessing this information. As for the authentication software it depends on which architecture or identity model is supported, in case it is an older model with older authentication software it will be necessary to get an Identity Manager, e.g. from SUN. But if a company is going to use new technologies it must certainly support software that backs up a user-centric approach, like MS cardspace, OpenID and Higgins.

30 http://www.demorgen.be/dm/nl/nieuws/multimedia/473019 accessed June 2007

Trust broker functionalities	Technology	Note
Identification	OpenID	Creates a decentralized identity management system, that will let you use multiple identities.
	MS Cardspace	Creates a simple front-end system to choose your identity. Made possible by the identity meta-system of K. Cameron.
	Higgins	Open source project to create a true platform- and protocol independent framework for a secure identity infrastructure.
	XRI	XRI is a true RESTful[31] approach. XRI is a universal identifier for all entities across multiple domains or directories.
Reputation monitoring	Jyte, eBay and Experian	A combination of these technologies with additional functions for analyzing information collected by the accounting process.
Behaviour monitoring	Link-contracts (XDI)	As a sub-part of XDI, link-contracts make it possible to monitor a digital contract by giving the owner active control.
	Ws-agreement	This protocol enables to create, specify and manage an agreement with other parties.
General technologies	Ws-security (WSS)	Specifies how integrity and confidentiality can be enforced in Web Services messaging.
	Ws-policy	Makes it possible for web-services to advertise a policy through XML.
	Ws-trust	Makes it possible to create, exchange and validate different security tokens by using the security mechanism from WSS.
	Ws-federation	Specifies a mechanism to allow different security domains to federate.
	ID-WSF	ID-WSF is a framework that works with specific open standards and protocols to ensure web-service security.
	ID-FF	ID-FF is a framework based on open standards and specifies how to make a secure, multi-vendor federated network.
	SAML 2.0	SAML promotes interoperability between disparate security systems, providing the framework for secure e-business transactions across company boundaries.

31 http://www.xfront.com/REST-Web-Services.html accessed June 2007

10. Is the Trust broker Framework feasible?

Now that we have established which functions the Trust broker will deliver, how to perform these and which technologies will be used to support these functions, it is time to evaluate this proposal. The Trust broker will play an important role within the context of de-perimeterization. The nature of the benefits will be focused to the business areas. From a technical perspective the Trust broker will not deliver any shocking new functionalities. This derives from the fact that the Trust broker framework will transfer all existing services into a more secure and easier to manage environment. Due to this framework organizations will stimulated to harden the security measures between their services, also called re-perimeterization. This will be the first big step to towards de-perimeterization. But in order to fulfil the benefits of the Trust broker framework some problems will have to be overcome. Presently the technical problems will deliver the most difficulties. This is because most technical solutions are under development and are not yet tested or fine tuned for compatibility with other protocols. However with the high industrial pressure to solve much of these issues this will be completed in the near future. Another technical problem will be the development of the necessary software applications, such as the reputation and the behavioural software. This problem will have coherence with the future research in this area, as to how the requirements of each trust level are measured, and how trust levels are created and used. Determining the requirements and providing ways to solve this problem will be de most difficult to tackle. From a business point of view there will be only one minor difficulty to overcome. By creating a Circle of Trust and a Trust broker framework the total expenses will increase. This can lead to resistance from within the circle of trust or the organization itself. So it is crucial to research the cost and risk reductions on implementation of these models.

Overall, the problems in comparison with the possible benefits, that arise when using the Trust broker, I have to say that the combination of a Circle of Trust model with a Trust broker framework will be a viable proposal.

Reasons	Advantages	Disadvantages
Circle of Trust	Can act as an liability shield.	Creates additional expenses.
	Increases trustworthiness behaviour between transacting parties, by means of enforceability.	An additional governing entity that creates more paperwork.
	Can share costs over members, with an exception of the Centralized Model.	
Trust broker Framework	Creates a loosly-coupled platform to provide services.	To implement an organizations network architecture must be restructured.
	Increases business flexibility by creating a way to simply adding or updating services.	

11. Conclusion

To answer the question with which I started the document; what kind of role does a Trust broker have in a Jericho network environment? The Trust broker will make it possible to create digital trust between companies. With this digital trust all kinds of data sharing and or additional services will be made available between partners. The digital trust will be based on the 'real world' trust, by means of four topics:

1. Identity
2. Reputations
3. Behaviour
4. Control

To accomplish these four points technical and non-technical implementations are used.

Identity is largely done by the authentication module. However in order to make it universal available to other companies maybe new techniques are used for additional identification, such as the user-centric model.
Reputation service for how it has to be done do not yet exist, but there are some very good initiatives on the market, like experian, jyte and the eBay feedback system. In combination with their own accounting information and perhaps external sources there can be made a good decision about someone's reputation.
*Behaviour*al is in fact very close to reputation service, but more actual, it scans the present. Behaviour will be mostly monitored according to the obligations a person has to fulfil to this specific company.
Control is given by the law. So in order to give companies good legislative control an contractual framework have to be used. This is given by the Liberty Alliance in their creation of Circle of Trust. These circles can be made in three different models, a collaborative, consortium and a centralized model.

These subjects that shall be performed by the Trust broker, will establish trust between partners. Since trust is most important in relation with other partners, the Trust broker will handle all external traffic. But in order to act in this manner it will be required to do a lot more, like authorization, key management, et cetera. This will make the Trust broker too 'powerful', so segregation of duties must be applied. This can be done by creating a Trust broker framework. This framework can control and co-operate with every module, but it will not 'own' or influence these modules. By not giving the Trust broker full control it will not be able to perform more then two operations within a transaction. The segregation of duties concept also makes it robust because modules can easily be updated or replaced. Furthermore the Trust broker will not become a single point of failure because all the modules will continue to work if the Trust broker fails, but they will not communicate in a trusted and secure manner with the outside world. In conclusion, the Trust broker will become a gateway between the real world and the digital realm by delivering secure services to the whole world. It will introducing legislative control to the digital realm and establishes ways to monitor entities and contracts to the real world. However, because of the present maturity level of the solutions needed to implement a Trust broker, it is not possible yet. Nevertheless these developments are going more rapidly every day, so within months possibly a few years implementation will be possible and de-perimeterization will definitely happen.

Future research

First of all, a question that was constantly on my mind during this project was, how the balance between security and privacy should be. This subject has always been a point of discussion, but since 9/11 and the increasing threat of terrorism it is more current then ever. I ask this question because the Trust broker actually wants to know as much as possible about an entity, but how does this harm the privacy of that entity? An interesting proposal is made by Wouter Teepe in his phd. Thesis 'Reconciling information exchange and confidentiality', he tries to give some theoretical and practical solutions in this area of tension between privacy and security. Second point of research will be about trust levels and data mining. The Trust broker now is made to collect and monitor data and the behavioural and reputation software will handle this information. But when this information has been processed the Trust broker will have to make connections and logical conclusions with this information, by performing some kind of data mining. Ultimately the Trust broker will have to give an entity a specific trust level. By means of these trust levels policies can be applied to the network environment. This can be compared to the use of DEFCON in the U.S. Military. DEFCON displays the state of readiness of the army, in case of an higher DEFCON level the security measures taken will be much higher then when it has an lower DEFCON level.