The road to Jericho

The Masters Series

Jericho in depth…

The road to Jericho

Enables organizations to migrate to a Jericho based network

Alina Stan

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

.

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 The sudden boost of Internet technology over the past decade does not fit well with our outdated design principles for network security.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

Contents

Phase A: Architecture Vision

- One iteration of the architecture process that sets the:

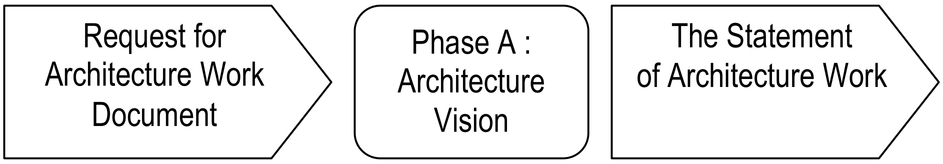
  Scope
  Constraints } of the project
  Expectations

- Validation of the business context
- Statement of Architecture work

Purpose

The aim of this book is to design, evaluate and build an IT security architecture for the organizations that want to adopt the Jericho principles and migrate to an Jericho enabled network. The Jericho enabled IT security architecture is designed in conformity with The Open Group Architecture Framework™ (TOGAF). For developing this security architecture, the Architecture Development Method™ (ADM) specified in TOGAF will be employed.

The development process of the Architecture Vision Phase:


Request for Architecture Work Document
Phase A : Architecture Vision
The Statement of Architecture Work

Vision

A "generic" security architecture based on the Jericho Forum Commandments and on the changing business requirements will be designed and evaluated against the requirements for a Jericho enabled network. This security architecture will serve as a "reference" model for the organizations that will migrate to a Jericho enabled network. The Jericho security architecture represents a business oriented security solution that supports and enhances the security of the organizations that perform mainly electronic transactions in a collaborative environment. The Jericho security architecture comprises an effective security solution for Jericho networks that protects against actual threats, is scalable, robust and proposes interoperability as a defining characteristic. This security architecture will provide the framework and foundation to enable secure communications & trust brokering services, and to protect the business processes and sensitive information of the adopting organizations. Besides these, the architecture will identify the security services that address the topics of interest (e.g. authentication, authorization, digital rights management, trust brokering services, secure communications, endpoint security etc.) determined by Jericho Forum. The Jericho security architecture documents the planning and design of the Jericho enabled networks. It specifies the processes identified within Jericho networks, the recommended open standards and technologies for protecting the businesses that operate in an electronic environment, the best practices based on the Jericho Forum Commandments.

This architecture will enable the organizations to migrate to the Jericho based network.

Principles for the Security Architecture

- **Simplicity**: the architecture has to be easy to understand and manageable at the following levels: Business level, Information System level (data and applications), Technological level
- **Flexibility**, **scalability**, **adaptability**, and **maintainability** refer to:
  - The security architecture must continuously be adapted to the new requirements of the business and technical changes that reflect the de-perimeterization principle
  - The capacity to incorporate all the business and technical requirements and changes in the security architecture
  - This security architecture must lead to a flexible and maintainable Jericho enabled network
  - The security architecture contains independent processes and modules that are interdependent and generate exchanges based on their different functionalities
  - The architecture can be augmented with new security modules and services
  - The implementation of a process or module specified in the Jericho security architecture must allow efficient maintenance, making it is easy to add or modify functionalities
- **Holistic view of security**
  - Jericho Security Architecture offers a holistic view upon security. In Jericho based networks, security is applied in layers: secure the network, secure the host, secure the application and secure the data
- **Open Architecture**
  - It is fully disclosed for peer review, standardization, and adoption by the industry.

Data Security Architecture

According to the ninth Jericho Forum Commandment "Access to data should be controlled by security attributes of the data itself", so the security attributes of the data should be found in the data itself. Commandment number eleven states that "By default, data must be appropriately secured when stored, in transit and in use". Also, the issues of data protection and control is discussed in the position paper "Enterprise Information Protection & Control (Digital Rights Management)" published by Jericho Forum in October 2006. In Jericho networks the access to sensitive data, as well as the access rights of the user upon the data are controlled and established through a dynamic authorization process in combination with the feedback and validations obtained from the interactions of all the security mechanisms in place. Sensitive data might include credentials used for authentication, or data such as credit card numbers, or bank transaction details, patient healthcare information. Defining what sensitive data is depends on the security policy of each organization and on the security levels attached to data (e.g. confidential, secret, top secret). In fact, the protection and control of the data is based on a joint result of the authentication, authorization, accounting, endpoint security, data classification, and encryption processes. In Jericho networks, data protection and control should be governed by a security policy that is further enforced by security mechanisms implemented by the other processes mentioned above. Moreover, before a user or an entity may act upon the data, a series of validations and interactions between the processes will take place.

- Based on the combination of the authentication method and the endpoint security status, a certain trust level of the user environment is created and assessed. The user can access the data if it reaches at least the trust level required by the security attributes attached to the data.
- Based on the authentication context and on the retrieved information status regarding the endpoint security, the users will be assigned a certain access level and corresponding access rights.
- The data has to be classified according to its sensitivity to loss or disclosure and has to reflect the requirements of the business processes and the security policy.
- A data classification policy is created, including the assigned access levels. Also, the accepted levels of behaviours and privileges that the users might have when accessing and handling the different types of data should be specified by the policy. Consequently, security classification levels that indicate the level of sensitivity associated with data, and define the acceptable use of data should be established.
- The technological solution for data classification in Jericho networks has to classify automatically the enterprise data in different security levels based on the adopted data classification policy.
- Also, security controls should be in place for administering the access requests to the data, monitoring and logging the access and executed operations upon different types

of data, enforcing the privileges and rights different users might have with respect to a data type.

- According to the security level assigned to data (e.g. confidential, secret, top secret), different cryptographic protocols and algorithms can be selected for protecting the data in transit.
- Accounting information and metadata regarding the data classification, data usage and handling should be stored for auditing, control and analysis activities.

In Jericho security architecture a multi-level security (MLS) model can be used. The main goals of MLS are:

- First, establish controls that prevent users from accessing information at a higher classification than their authorization permits; and
- Second, ensure that the controls prevent unauthorized users from declassifying information or accessing information for which they don't have enough rights

The effective implementation of MLS systems ensure that data can be consolidated onto a single infrastructure, while maintaining the highest levels of assurance that it can only be accessed by authorized users. The MLS systems will support a greater measure of data dissemination between different entities, along with a high level of assurance. MLS ity functions include: data classification, auditing, user identification and authorization, name hiding of files that cannot be accessed by a certain user. MLS inserts security tags into the data stream to control access and audit usage.

Application Security Architecture

An enterprise contains different applications, web services, web applications, databases existent in a company that contain sensitive data and confidential users' information. The Application Security Architecture within Jericho security architecture aims to provide a series of guidelines for assessing and securing the applications in an enterprise. These guidelines and principles have to be used at the design, development and use of the applications in an enterprise. Besides these, the Application Security Architecture will provide a set of best practices regarding the development and use of existent and new applications. In fact, application security refers means managing the risks and vulnerabilities and implementing the countermeasures. The Application Security Architecture occupies a central role in Jericho Security Architecture and refers to:

- Secure business collaboration
- Security for all the applications, databases and Web services existent in an organization

Application Security Architecture includes:

- Authentication
- Authorization
- Audit and logging
- Application security integration
- Depends also on:
    - Endpoint security
    - Secure communications : End-to-end encryption and end-to-end security[1]
- XML Security : XML Encryption and XML Signature
- Secure Web services

Possible steps in securing the applications are:

- Threat modeling in application's design phaseSecure coding techniques have to be applied by developers for developing secure, robust, and hack-resilient solutions
- The design and development of application layer software must be supported by a secure network, host, and application configuration on the servers where the application software is to be deployed.

Possible solutions for application security are:

- XML security gateways
- Web application firewalls
- Web application penetration testing
- Products and services for evaluating the application source code; validation of secure coding for applications
- Federated identity
- Database security
- Identity Federation

Benefits of Application Security

- Lower cost of recovery and lost productivity
- Minimize loss of data
- Improve customer confidence
- Decrease legal risks

[1] Security is best when designed and implemented end-to-end

Phase B: Business Architecture

In this Phase we will describe the Business Architecture "As Is" (the baseline) and the "To Be" Business Architecture from the Information Technology and Security points of view. Basically, in this phase there is defined the business case for a new security architecture.

Business Drivers

Firstly, several important business drivers have been identified that demand for a new view of security:

- Globalization, digitalization and personalization are changing the way business is done today and forever
- Wider collaboration between organizations outside their perimeters is required due to the explosion of pervasive, fast, reliable, and cheap Internet connectivity
- Collaborative business environment for electronic commerce; new work patterns emerge
- New business models based on electronic transactions and mobile users that connect the organizations and their business processes to all external stakeholders, sustain collaboration anytime, anywhere, at low costs among all the entities have emerged
- The need for trust models within the business partnerships among different organizations
- Business mergers and acquisitions (extended organizations) that generate new services; requirements for shorter time to market, business agility

Business Needs	"As Is" Now	"To Be" Target
Need to exchange data	Data available on hosts, everywhere on user's systems	A central data server that controls the access to the data depending on the authentication and authorization level
Need Internet access	Unrestricted Internet access from the endpoints	Unrestricted Internet access from controlled and secured endpoints
Need to access applications	Applications are accessible on endpoints or on intranet servers	Develop applications and systems that are Internet enabled and accessible through the use of Web services. Adequate security controls such as transport layer security, message layer security, authentication and authorization should be employed.
Need remote access	Remote connections are allowed to intranets	Implement Web based access for applications and employ adequate security controls that protect the access to resources (e.g. services, data)
Business partners need access to the applications and resources	VPNs, different e-commerce applications	Access based on the checking of the endpoint security, authentication and authorization of the 3rd parties Employ security controls that are more application centric and data protection centric.
Protect the corporate network	Network hardening technologies were employed (firewalls, VPNs, NAT)	Employ security controls that are more application centric and data protection centric. Moreover, adequate authentication and authorization of the entities, endpoint security mechanisms should be used. Data classification, encryption, DRM, time stamping should be performed where necessary.
Need of electronic commerce/collaboration and transactions; value chain oriented businesses	VPNs, Web sites, Web applications and standards (e.g. SET)	Web Services, SOA, open and inherently secure standards

Business Needs	"As Is" Now	"To Be" Target
Need to be able to handle high volumes of users (intern & extern)	Different identity management systems that are not interoperable, nor able to meet the increasing needs to handle to hand so many users	Federated identity management system or user-centric identity management system. Anyway, the chosen identity management system has to be efficient in terms of resources used, and also scalable for increasing number of users
Adequate security that is cost effective and enables business agility; timely access to the resources also for the business partners	The traditional ways of protecting the corporate network are not scalable and do not provide the desired security level protection for the asset at risk	JFC #1[1] The scope and level of protection should be specific & appropriate to the asset at risk. Identification of the most important assets (e.g. applications) in a network and focus on their adequate protection. Individual systems and data will be capable of protecting themselves.
Need for Trust Models among business partners	Different contracts and agreements among parties, certificates	The Trust Broker framework comprises functions for checking the credentials of the entities, building reputation based on the behaviour patterns, manages and maintains trust based relationships online Enforcement of the contracts and agreements among entities

Bases on the drivers and business needs mentioned above, it can be concluded that a new security architecture and design approach are required for enabling businesses to grow safely and securely in an open, Internet-driven, de-perimeterized network.

[1] Jericho Forum Commandments Version 1.2 May 2007

Phase C: Information Systems Architectures

The focus in a Jericho based network is on preserving the integrity, reliability, availability, confidentiality of sensitive information while protecting the applications' functionalities. The most effective way to protect information and systems is to incorporate security into each domain of the enterprise architecture. In this way, the security services support the applications' functions, thus facilitating the business operations.

Technical drivers

New technical drivers that enable businesses to collaborate & co-operate have emerged:

- Resources almost without limits (etc. Internet connectivity, Storage, Grid Computing, pervasive computing/ubiquitous computing)
- Emergence of mashup corporations: Service Oriented Architecture[1] (SOA) and Web Services
- Social software that enable collaboration: Web 2.0, Blogs, Forums, Virtual team spaces Wikis etc.
- Increased complexity of the actual architectures and systems
- Security's role as a business enabler increases and becomes widely recognized
- Security becomes challenging and complex to manage in a collaborative environment, so, a shift in the way security is implemented is emerging

Applications Principles

- Application Software should be independent from a specific hardware and operating systems software
- The use of SOA for achieving the interoperability and flexibility requirements for Security Architecture's vision and the business needs.
- The use of Web Services within the applications. So, the applications are organized into modular services that are typically web based. The use of Web Services enables interoperability between different applications independently from the technologies used.

[1] SOA is an approach to build distributed systems that deliver application functionality as services to end-user applications or to build other services. SOA represents an IT framework that combines individual business functions and processes, called *services*, to implement sophisticated business applications and processes.

SOA is a style of design, deployment, and management of software infrastructure and applications.

- The use of adequate communication protocols that provide interoperability and transparency for invoking and accessing the services
- Well defined and trusted interfaces for services interactions
- The solutions for the enterprise applications are a combination of services and services interactions
- Simplification of the processes; integration and implementation of the processes as services

Benefits for using SOA for the applications and software infrastructure:

- **Business and IT flexibility are achieved:** a more flexible enterprise architecture that is designed for continuous business change. The configuration of loosely coupled services is simple, fast and low-cost
- **The services are widely available for all categories of users:** the access to the services is facilitated for the users
- **The businesses and their processes become digital:** the new business requirements are reflected in the IT. The technology offers support and mirrors the changing business requirements.
- **Cost Savings:** Organizations implementing SOA have the potential to achieve significant cost reductions by *reusing sharable business services*, rather than recreating functionality to address the needs of each application initiative. SOA simplifies and accelerates application development, which enables organizations to do more with less.
- **Aligning IT to Business Processes:** SOA transforms IT systems into self-contained services that accurately reflect business processes and operational requirements. With SOA, IT mirrors business operations, which improves the utility IT delivers to the business.

Security Services

The following security services will be attained in a Jericho enabled network:

- **Confidentiality:** refers protecting the data against attacks conducted by unauthorized entities and ensuring the privacy of sensitive data
- **Integrity:** means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity
- **Authentication of the entities**
- **Availability**: means that the resources needed to achieve the security requirements imposed by Jericho Security are always ready to be used. In the context of communications over Internet, this means that whenever information

needs to be transmitted, the communication channel is available and the receiver can cope with the incoming data. In the context of endpoint security, this means that the agents that perform security checks on the endpoint can provide security status whenever is needed.

- **Accountability**: at the individual level

All these security services are required in a network based on the Jericho commandments.

Requirements for Jericho Security Architecture based on Jericho Forum Commandments

Moreover, the security services have to fulfil also the requirements derived from Jericho Forum Commandments:

1. **The scope and level of protection should be specific & appropriate to the asset at risk.**
   - **Cost effective**: The chosen security solutions should reduce the costs of providing security for the asset at risk
   - **Self-protection mechanisms**: The assets and the data have to contain mechanisms (e.g. security attributes, security controls) for protecting themselves
2. **Security mechanisms must be pervasive, simple, scalable & easy to manage**
   - **Simplicity**: The chosen security solutions should reduce the complexity of the architecture, while improving the security and decreasing the administrative efforts
   - **Scalability**: The security solutions must be able to operate on a global scale and offer protection for al the critical assets and sensitive data on the network
   - **Interoperability**: The chosen solutions should be interoperable on a large scale in a collaborative environment
3. **Assume context at your peril**
   - **Flexibility**: The chosen solutions should be flexible and be able to operate in different environments
4. **Devices and applications must communicate using open, secure protocols**
   - **Open protocols**: The security solutions for Jericho architecture have to be based on open standards and protocols that are widely accepted.
5. **All devices must be capable of maintaining their security policy on an untrusted network**
   - **Complete security policy**: Comprehensive security policies for protecting the network assets in an Internet environment have to be used in a Jericho enabled network.

6. **All people, processes, technology must have been declared and transparent levels of trust for any transaction to take place**
   - **Trust context, contracts and levels**: Different trust levels are established and entities interact in a certain trust context in a Jericho enabled network. The transactions on the network are specified by trust contracts.
7. **Mutual trust assurance levels must be determinable**
   - **Mutual trust levels**: Trust levels are assigned to entities (users, devices) depending on results from the authentication and authorization processes.
8. **Authentication, authorization and accountability must interoperate / exchange outside of your locus / area of control**
   - **Interoperability**: The chosen solutions for authentication, authorization and accountability, and not only, should be interoperable on a large scale for different trust contexts and transaction models over the Internet.
   - **Trust broker services**: A system should be in place for establishing trust contexts between entities, evaluating and assigning trust levels in a collaborative environment. The Trust broker system will control access to resources, the rights and privileges of the entities in a multi-level security and trust environment.
9. **Access to data should be controlled by security attributes of the data itself**
   - **Multi-level security**: The data and the entities are classified according to a multi-level security model. The data attributes, content, context and sensitivity to loss or disclosure are the factors used in classifying the data. The evaluated trust level of an entity, along with the trust profile, authentication method etc. are factors that help in classifying the users and assigning them corresponding privileges.
10. **Data privacy (and security of any asset of sufficiently high value) requires a segregation of duties/privileges**
    - **Segregation of duties**: Limiting the access, the rights and the privileges of the users to the data and to the systems. No single individual can have control over all phases of a transaction. Security controls must be also used where necessary for enforcing the separation of duties/privileges.
11. **By default, data must be appropriately secured when stored, in transit and in use**
    - **Multi-level security model**: The use of different methods of protecting the data (e.g. encryption, message digests, security controls etc.) according to the assigned data security level (e.g. sensitivity to loss or disclosure).

In conclusion, Jericho Security Architecture will provide defence in depth, at different layers of protection of the data, applications, systems, endpoints and, finally, the network itself.

Phase D: Technology Architecture

If till now the role of IT was to automate the business processes and operations, nowadays it also has to automate business-to-business and customer-to-business transactions and processes. Moreover, the collaborative business models require a different approach of the networks' infrastructure and security. The new network infrastructure and the way security is provided are based on the concept of de-perimeterization.

The corporate networks and systems will be opened for the outside world and this requires a new security architecture that offers the means to protect adequately and efficiently the corporate assets (e.g data, services).

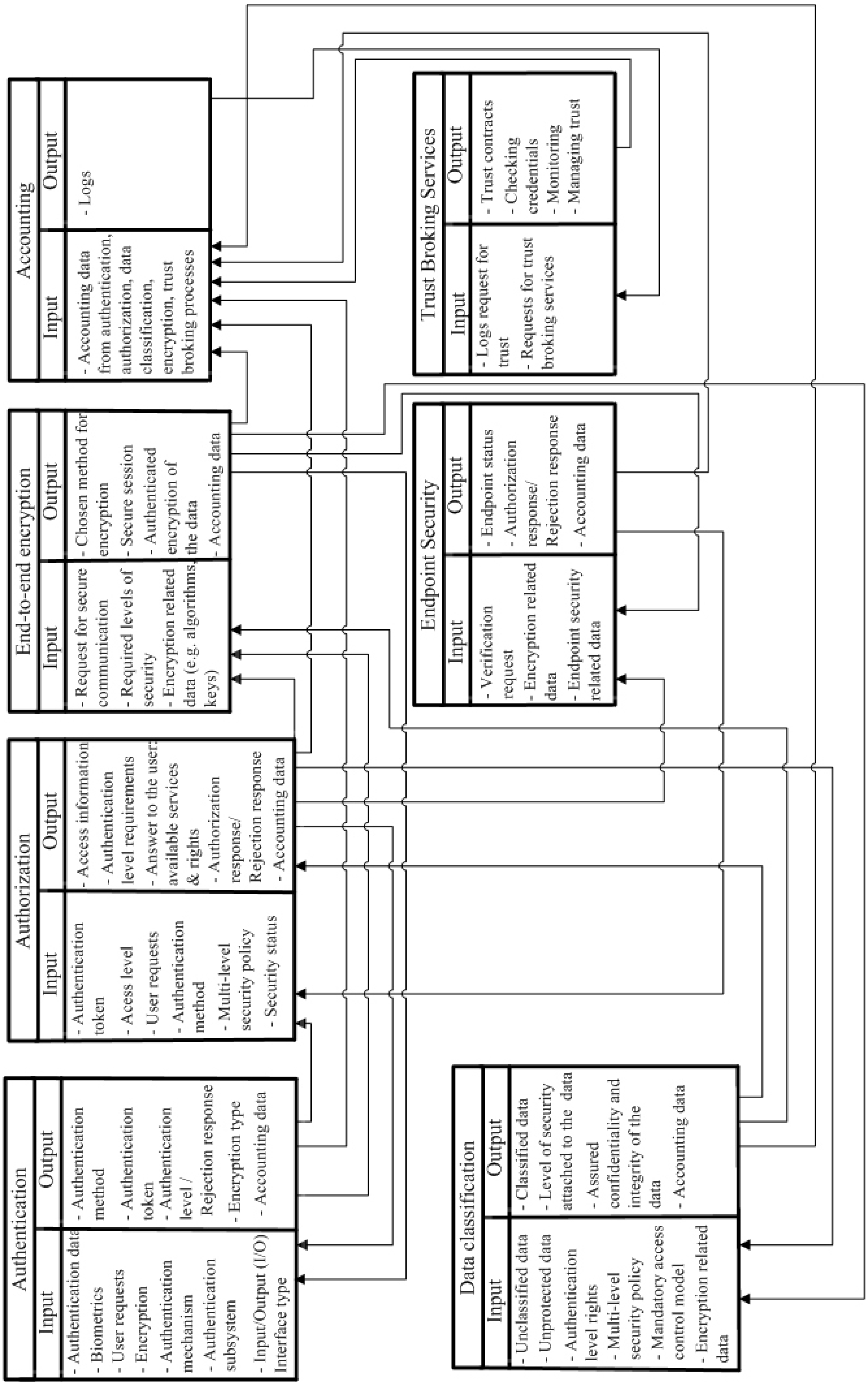
In a Jericho based network, the following processes/modules have been determined in order to adequately protect the critical assets of the corporate network:

- Authentication
- Authorization
- Accounting
- Endpoint security
- Data classification & data leakage
- Secure communications: end-to-end encryption
- Trust Broker Framework

Next, the inter-relationships and interactions between the above mentioned modules are specified:

	Authentication	Authorization	Accounting	Endpoint Security	Data Classification	End-to-end encryption	Trust Broker Framework
Data Classification	• Receives authentication information when data is accessed, retrieved etc.	• Receives as input a multi-level security policy • Uses a mandatory-access level model	• Provides accounting data	• Provides reports about the data classification method		• Request for encryption related data (e.g. algorithms, keys, protocols) needed for different security levels assigned to the data	• Requests data as input for determining the security levels assigned to different data
End-to-end encryption	• Provides encryption related data (e.g. algorithms, keys, protocols)	• Provides encryption related data (e.g. algorithms, keys, protocols)	• Provides accounting data	• Provides encryption related data (e.g. algorithms, keys, protocols)	• Provides encryption related data (e.g. algorithms, keys, protocols)		• Provides encryption related data (e.g. algorithms, keys, protocols) upon request, based on trust level and security level
Trust Broker Framework	• Receives data for establishing trustworthiness (trust levels & contracts)	• Provides information from the security policies & contracts to the authorization process to decide about the rights and clearances	• Receives information for determining the trust levels • Provides info about contracts, which services, policy and maybe which identity per transactions • Provides info about which sources are used for determining the trust level	• Request reports about the compliance of entities with contracts and security policies	• Provides data as input for determining the security levels assigned to different data	• Request for encryption related data (e.g. algorithms, keys, protocols) needed for different security and trust levels	

	Authentication	Authorization	Accounting	Endpoint Security	Data Classification	End-to-end encryption	Trust Broker Framework
Authentication		• Provides the result and method of the authentication for the authorization process	• Provides accounting data	• May request endpoint status information	• Provides authentication information of the user	• May request encryption related data (e.g. algorithms, keys, protocols)	• Provides essential data for establishing trustworthiness (trust levels & contracts)
Authorization	• Requests the Authentication method • May require a user to be re-authenticate (in different context)		• May request user audit information • Provides accounting data	• May request detailed information about the endpoint security status	• Provides a multi-level security policy for data classification • Reads data classification metadata	• May request encryption related data (e.g. algorithms, keys, protocols)	• Requests information from the security policies & contracts for deciding about the rights and clearances
Accounting	• Authentication event is logged	• Authorization event is logged		• Security state change is logged • Reports of the security status scans	• Data decision classification is logged	• Request for secure communication is logged. • Secure communication parameters are logged	• Provides information for determining a trust level • Stores information about generating the contracts • Stores information about the sources that are used to determine a trust level
Endpoint Security	• May provide authentication information upon request (e.g. PKI, reputation)	• May provide status information upon request • May provide an authorization response/ rejection response	• Provides accounting data		• May request reports about the data classification method • May check the data classification process	• May request encryption related data (e.g. algorithms, keys, protocols)	• Provides status information and reports about the compliance of an entity with a contract or policy



Accounting	
Input	Output
- Accounting data from authentication, authorization, data classification, encryption, trust broking processes	- Logs

End-to-end encryption	
Input	Output
- Request for secure communication - Required levels of security - Encryption related data (e.g. algorithms, keys)	- Chosen method for encryption - Secure session - Authenticated encryption of the data - Accounting data

Authorization	
Input	Output
- Authentication token - Acess level - User requests - Authentication method - Multi-level security policy - Security status	- Access information - Authentication level requirements - Answer to the user: available services & rights - Authorization response/ Rejection response - Accounting data

Authentication	
Input	Output
- Authentication data - Biometrics - User requests - Encryption - Authentication mechanism - Authentication subsystem - Input/Output (I/O) Interface type	- Authentication method - Authentication token - Authentication level / Rejection response - Encryption type - Accounting data

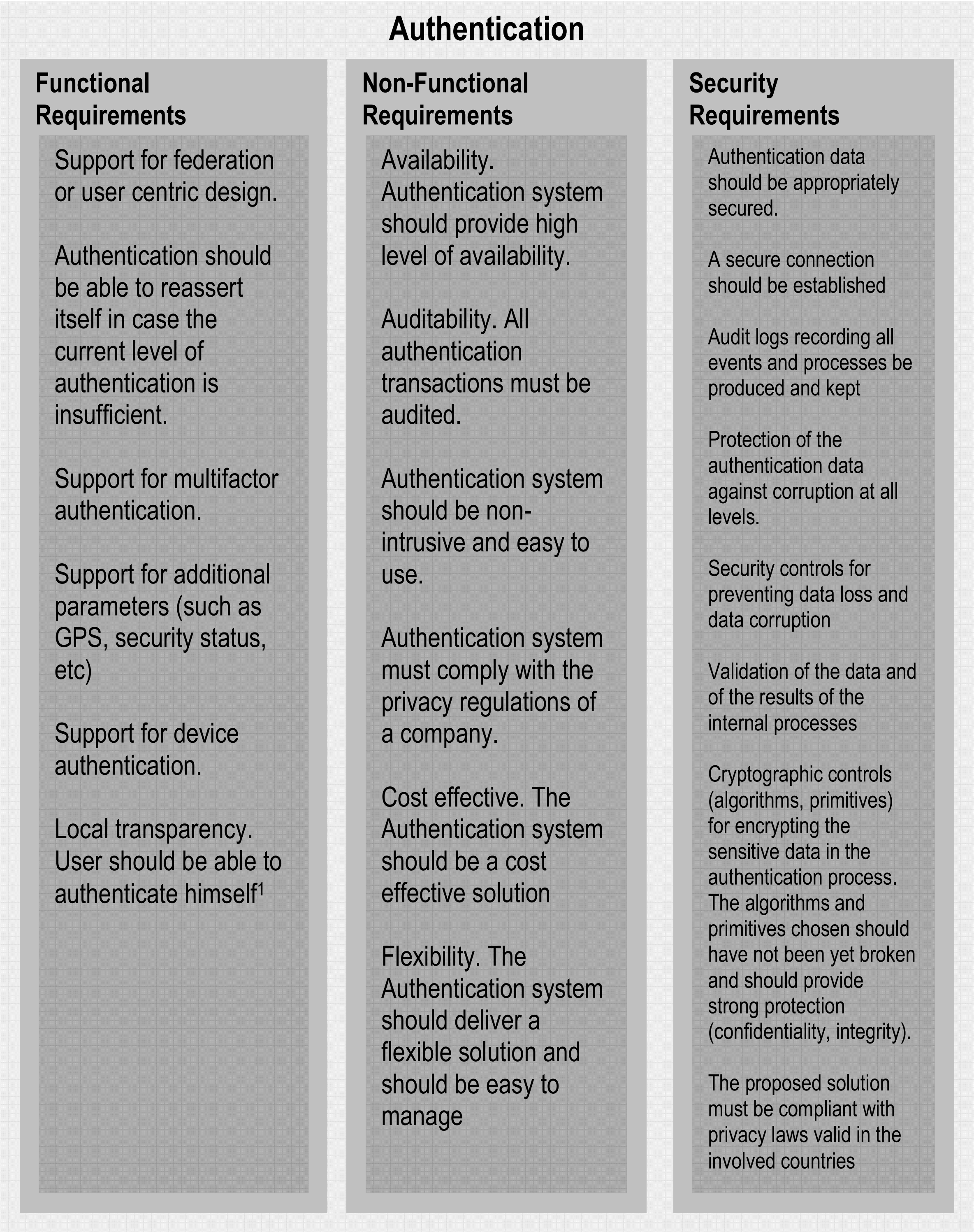
Trust Broking Services	
Input	Output
- Logs request for trust - Requests for trust broking services	- Trust contracts - Checking credentials - Monitoring - Managing trust

Endpoint Security	
Input	Output
- Verification request - Encryption related data - Endpoint security related data	- Endpoint status - Authorization response/ Rejection response - Accounting data

Data classification	
Input	Output
- Unclassified data - Unprotected data - Authentication level rights - Multi-level security policy - Mandatory access control model - Encryption related data	- Classified data - Level of security attached to the data - Assured confidentiality and integrity of the data - Accounting data

Table 1: The inter-relationships between the modules of Jericho Project

Figure 2: Interactions between the Jericho Project modules



Authentication

Functional Requirements

Support for federation or user centric design.

Authentication should be able to reassert itself in case the current level of authentication is insufficient.

Support for multifactor authentication.

Support for additional parameters (such as GPS, security status, etc)

Support for device authentication.

Local transparency. User should be able to authenticate himself[1]

Non-Functional Requirements

Availability. Authentication system should provide high level of availability.

Auditability. All authentication transactions must be audited.

Authentication system should be non-intrusive and easy to use.

Authentication system must comply with the privacy regulations of a company.

Cost effective. The Authentication system should be a cost effective solution

Flexibility. The Authentication system should deliver a flexible solution and should be easy to manage

Security Requirements

Authentication data should be appropriately secured.

A secure connection should be established

Audit logs recording all events and processes be produced and kept

Protection of the authentication data against corruption at all levels.

Security controls for preventing data loss and data corruption

Validation of the data and of the results of the internal processes

Cryptographic controls (algorithms, primitives) for encrypting the sensitive data in the authentication process. The algorithms and primitives chosen should have not been yet broken and should provide strong protection (confidentiality, integrity).

The proposed solution must be compliant with privacy laws valid in the involved countries

Authorization

Functional Requirements

Support for federated identities

Authorization system should not only be able to read the file system permissions, but also metadata from the files.

Authorization should be able to take endpoint security, audit data and authentication context (e.g. authentication data, authentication method, location etc.) into account when an authorization decision is made.

Non-Functional Requirements

Auditability. All authorization transactions must be audited.

Cost effective. The Authorization system should be a cost effective solution

Flexibility. The Authorization system should deliver a flexible solution and should be easy to manage

Availability. Authorization system should provide high level of availability.

Security Requirements

Role based access control for users should be used in combination with the identity management system.

A secure connection should be established

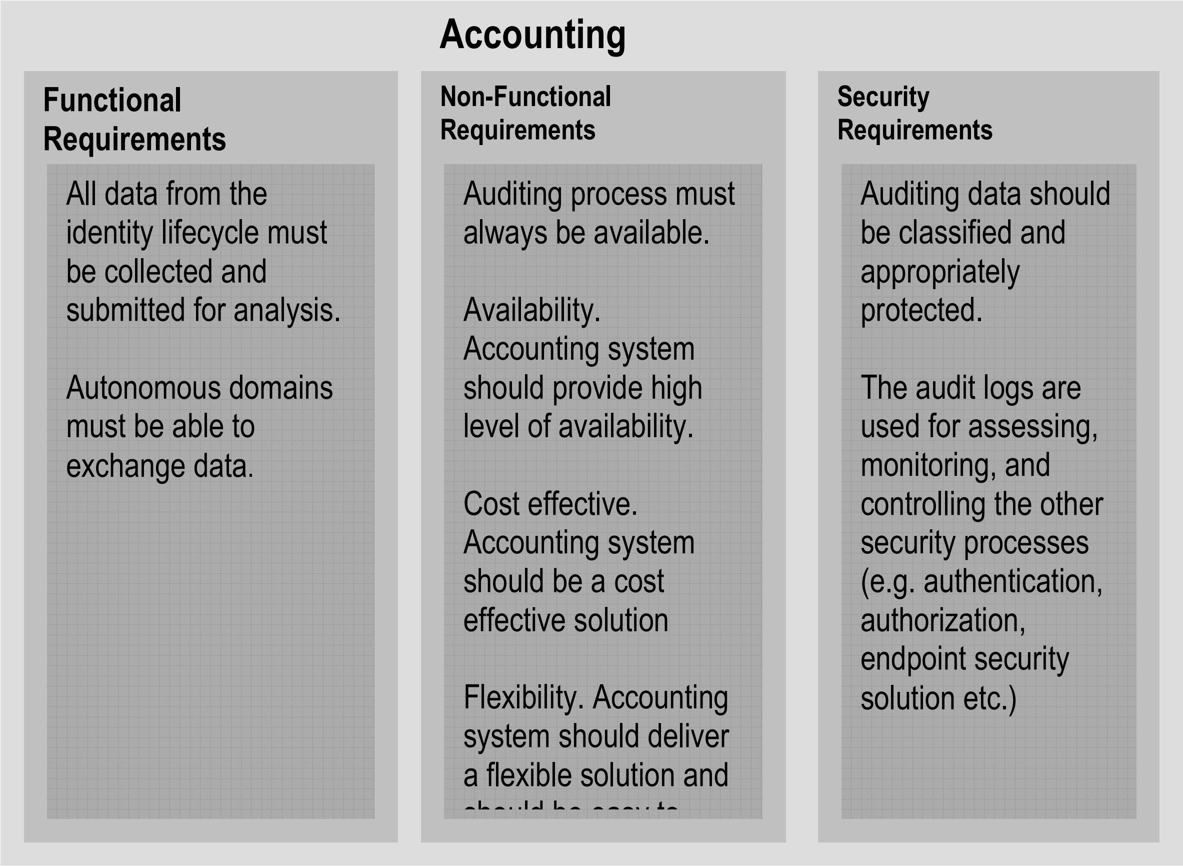
Cryptographic controls (algorithms, primitives) for encrypting the sensitive data in the authorization process. The algorithms and primitives chosen should have not been yet broken and should provide strong protection (confidentiality, integrity).

Audit logs recording all events and processes be produced and kept

Segregation of duties

Validation of the data and results obtained from the other processes (e.g. authentication, endpoint security etc.)

The proposed solution must be compliant with privacy laws valid in the involved countries.



Accounting

Functional Requirements

All data from the identity lifecycle must be collected and submitted for analysis.

Autonomous domains must be able to exchange data.

Non-Functional Requirements

Auditing process must always be available.

Availability. Accounting system should provide high level of availability.

Cost effective. Accounting system should be a cost effective solution

Flexibility. Accounting system should deliver a flexible solution and should be easy to

Security Requirements

Auditing data should be classified and appropriately protected.

The audit logs are used for assessing, monitoring, and controlling the other security processes (e.g. authentication, authorization, endpoint security solution etc.)

Endpoint Security

Functional Requirements

The chosen solution should be able to protect and assess the security status all the devices on the network

The chosen solution should retrieve current information status about all the devices on the network

Interoperability. The Endpoint security solution should be able to provide information status for all sorts of devices on a network that operate in different environments

Scalability. The Endpoint security solution must be able to operate on a global scale, on any network device

Non-Functional Requirements

Auditability. All Endpoint security checks and reports must be audited.

Availability. Endpoint security solution should provide high level of availability.

Cost effective. The Endpoint security solution should be a cost effective solution

Flexibility. The Endpoint security solution should deliver flexibility and should be easy to manage

Security Requirements

Audit logs recording all events and processes should be produced and kept

Security patch management policy

Segregation of duties/privileges for preventing the modification of the settings and the status data of the Endpoint security solution

Cryptographic controls (algorithms, primitives) for encrypting the status data that is generated and transmitted by the endpoint security solution. The algorithms and primitives chosen should have not been yet broken and should provide strong protection (confidentiality, integrity).

The information status delivered by the Endpoint security solution should be expressed/reported in terms of security attributes.

A trust context is created and validated based on the security attributes delivered by the Endpoint security solution

Segregation of duties

Data Classification

Functional Requirements

Data should be dynamically classified according to its sensitivity to loss or disclosure with an automatic tool

The classification system has to take into consideration the file attributes, the content of the files, and the value of that data for the business

The classification system should be able to track and monitor the changes in the data and reflect these by dynamically classifying the data

Non-Functional Requirements

Auditability. All accesses to the data and the operation on the data must be audited.

Heterogeneous. The classification system has to support and recognize all types of files and data for classification

Scalability. It should scale for large amounts of data that can be located everywhere in the network

Availability. Data should be available for the users

Cost effective. The data classification system should be a cost effective solution

Flexibility. The data classification system should deliver a flexible solution and should be easy to manage

Interoperability. The data protection system should provide interoperability when protecting the data.

Security Requirements

Data is classified automatically in distinct security levels (e.g. public, confidential, secret, top secret)

The users will be assigned security levels (clearances) as well. The users are authenticated and authorized before having access to data

The multi-level security policy is used for classifying the data and the users.

Segregation of duties

Security controls for preventing data loss and data corruption must be used.

Audit logs recording all events and processes must be produced and kept

Security controls and triggers must perform validations of the data, administer & control the access requests to the data, the permissions on the data, the flow of the data (e.g. Bell La Pandula model no write down, no read up)

Automated corrective actions that enforce the privileges and rights of users and security notifications/alerts should occur if unauthorized access and handling of the data are detected

End-to-end encryption

Functional Requirements	Non-Functional Requirements	Security Requirements
Data in transit has to be adequately protected in terms of privacy and integrity	Cost effective. The end-to-end encryption solution should be a cost effective solution. Flexibility. The end-to-end encryption solution should deliver flexibility and should be easy to manage Interoperability. The end-to-end encryption solution should provide interoperability when protecting the data in transit from host-to-host Availability. The end-to-end encryption solution should provide high level of availability. Auditability. All accesses to the data and all the operations on the data must be audited.	A secure connection should be established The Authentication and Authorization processes have to occur before the data transfer begins Cryptographic controls (algorithms, primitives) for encrypting the sensitive data classified in multi-security levels. The algorithms and primitives chosen should have not been yet broken and should provide strong protection (confidentiality, integrity). Authenticated Encryption solutions (authentication of the entities prior to start communication; secure connection established; adequate cryptographic protocols and algorithms in accordance with the security (sensitivity) level assigned to data) Audit logs recording all events and processes must be produced and kept

Data Protection

Functional Requirements

All the data existent on the network should be adequately protected based on a multi-level security model and on trust levels

Where appropriate, users should be presented with views on the data depending on their rights

The protection and control of the data is based on a joint result of the authentication, authorization, accounting, endpoint security, data classification, and encryption processes.

Non-Functional Requirements

Auditability. All accesses to the data and all the operations on the data must be audited.

Cost effective. The data protection system be a cost effective solution

Flexibility. The data protection system should deliver a flexible solution and should be easy to manage.

Availability. The data protection system should provide high level of availability.

Scalability. It should scale for large amounts of data that can be located everywhere in the network

Heterogeneous. The data protection system has to support and recognize & adequately protect all

Security Requirements

Audit logs recording all events and processes must be produced and kept

The users and the data are classified based on a multi-trust level.

The users have to be adequately authenticated and authorized.

The endpoint security status is retrieved and validated

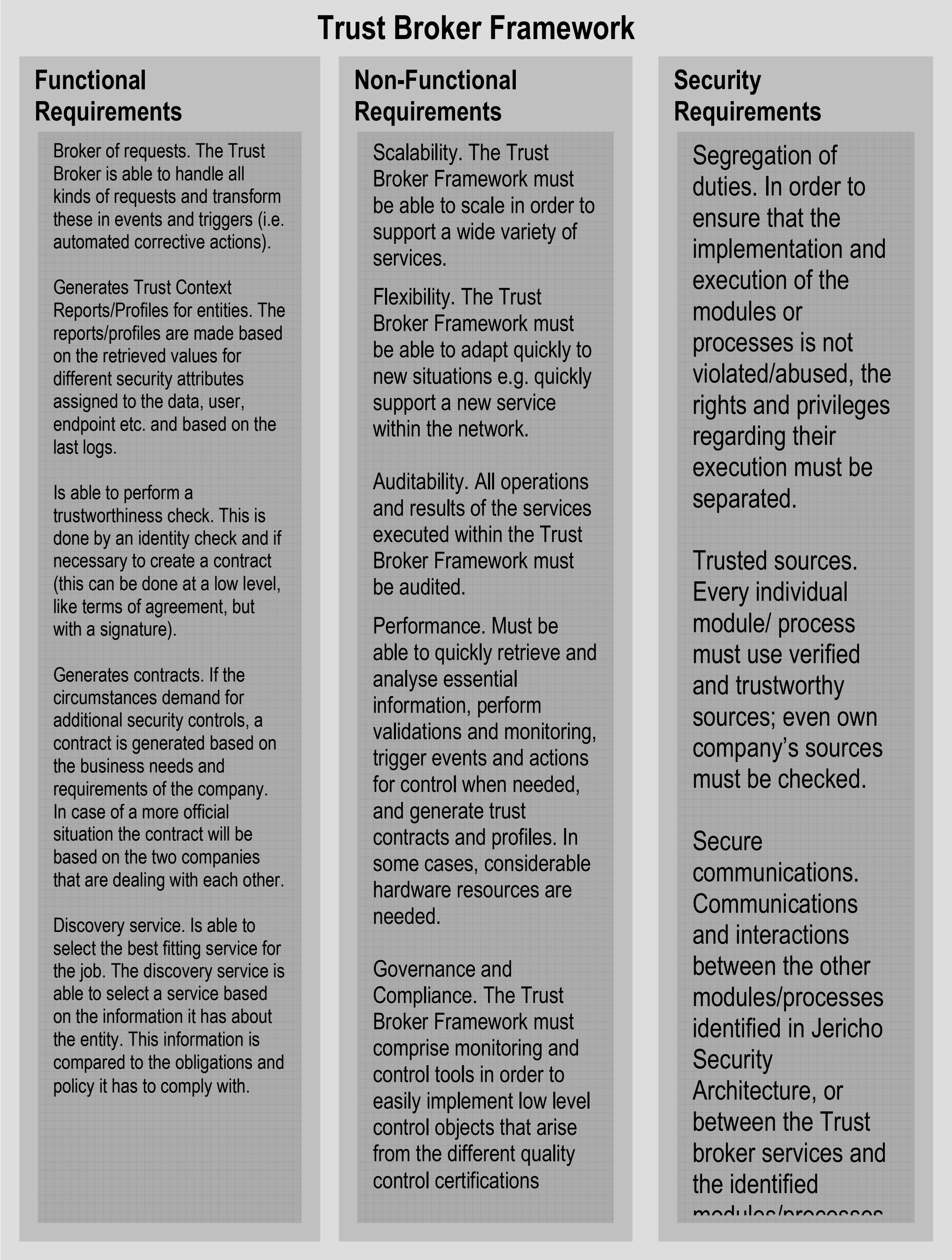
Based on the combination of the authentication method and the endpoint

Security controls and triggers must perform validations of the data, administer & control the access requests to the data, the permissions on the data, the flow of the data (e.g. Bella La Pandula model no write down, no read up)

Automated corrective actions that enforce the privileges and rights of users and security notifications/alerts should occur if unauthorized access and handling of the data are detected

According to the security level assigned to data (e.g. confidential, secret, top secret), different cryptographic protocols and algorithms can be selected for protecting the data in transit.

Segregation of duties



Trust Broker Framework

Functional Requirements

Broker of requests. The Trust Broker is able to handle all kinds of requests and transform these in events and triggers (i.e. automated corrective actions).

Generates Trust Context Reports/Profiles for entities. The reports/profiles are made based on the retrieved values for different security attributes assigned to the data, user, endpoint etc. and based on the last logs.

Is able to perform a trustworthiness check. This is done by an identity check and if necessary to create a contract (this can be done at a low level, like terms of agreement, but with a signature).

Generates contracts. If the circumstances demand for additional security controls, a contract is generated based on the business needs and requirements of the company. In case of a more official situation the contract will be based on the two companies that are dealing with each other.

Discovery service. Is able to select the best fitting service for the job. The discovery service is able to select a service based on the information it has about the entity. This information is compared to the obligations and policy it has to comply with.

Non-Functional Requirements

Scalability. The Trust Broker Framework must be able to scale in order to support a wide variety of services.

Flexibility. The Trust Broker Framework must be able to adapt quickly to new situations e.g. quickly support a new service within the network.

Auditability. All operations and results of the services executed within the Trust Broker Framework must be audited.

Performance. Must be able to quickly retrieve and analyse essential information, perform validations and monitoring, trigger events and actions for control when needed, and generate trust contracts and profiles. In some cases, considerable hardware resources are needed.

Governance and Compliance. The Trust Broker Framework must comprise monitoring and control tools in order to easily implement low level control objects that arise from the different quality control certifications

Security Requirements

Segregation of duties. In order to ensure that the implementation and execution of the modules or processes is not violated/abused, the rights and privileges regarding their execution must be separated.

Trusted sources. Every individual module/ process must use verified and trustworthy sources; even own company's sources must be checked.

Secure communications. Communications and interactions between the other modules/processes identified in Jericho Security Architecture, or between the Trust broker services and the identified modules/processes

Table 2: Requirements for the Jericho Project modules

Authentication

"As Is" Now	"To Be" Target	Results Jericho Research	Possible Technologies
Isolated domains In-depth trust relationship between the communicating parties.	Federated identity Level of trust is configurable	Federated and user centric design Authentication context defines the trust level	

Authorization

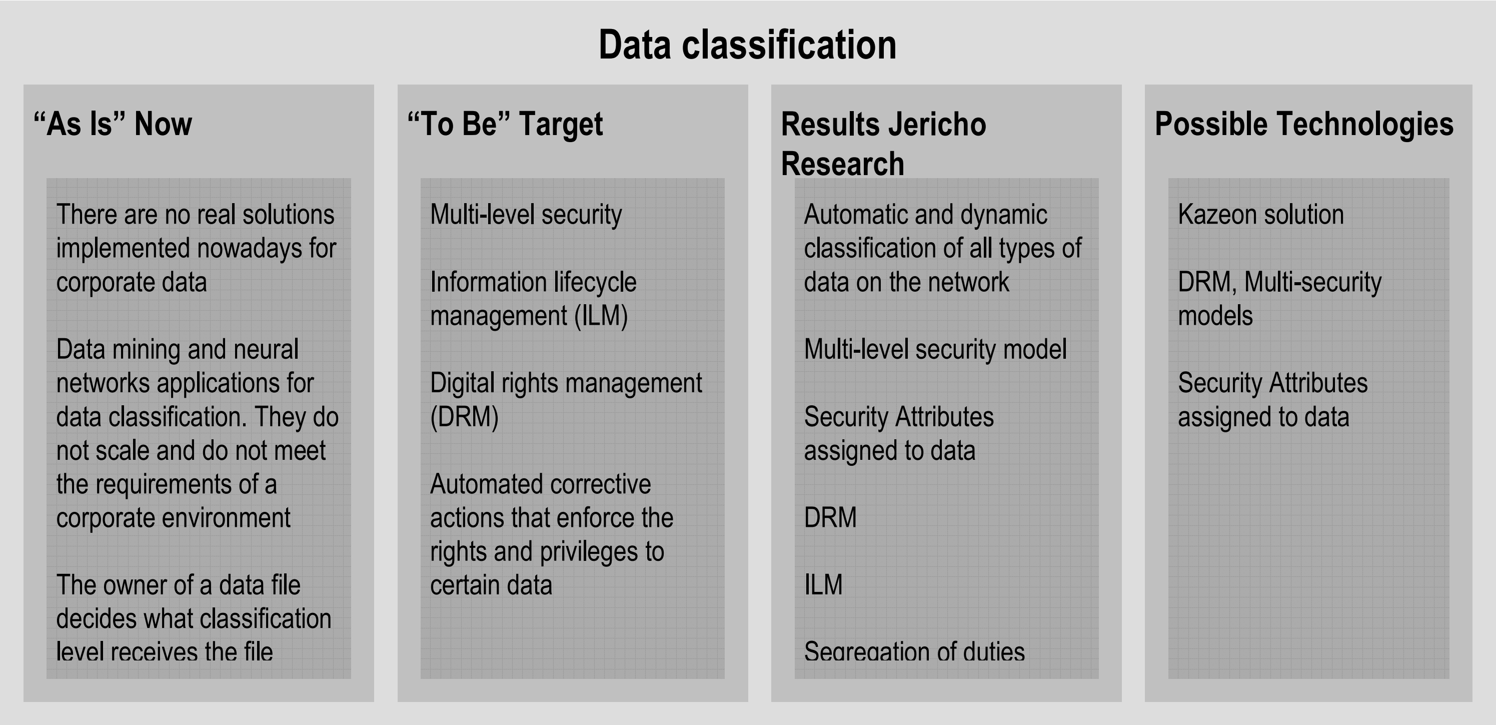
"As Is" Now	"To Be" Target	Results Jericho Research	Possible Technologies
Passive authorization model Discretionary access control	Role based access control; segregation of duties Mandatory access control Active authorization model Design of levels of trust based on the authentication method and on the security status of the endpoint Automated corrective actions that enforce the privileges and rights of users and security notifications/alerts should occur if unauthorized access and handling of the data are detected Mandatory access controls: Compare the clearances (security levels) of the subjects with the security levels assigned to data for establishing the rights and privileges of the users.	Assess the authentication context and the endpoint status information to create trust levels Active authorization and claim-based authorization systems	

Accounting

“As Is” Now	“To Be” Target	Results Jericho Research	Possible Technologies
Logs are spread over the local network Audit data is contained within a single domain.	Auditing spans multiple systems/domains Partial or complete audit data exchange between the collaborating parties.	Distributed auditing	

Endpoint security

"As Is" Now	"To Be" Target	Results Jericho Research	Possible Technologies
Non-interoperable solutions No comprehensive solutions	The security status of all devices on the network should be verified and validated upon requests Agents on each device that monitor end maintain the device's security Automatic patches of the security mechanisms that protect the devices Automated corrective actions that enforce the security patch management policy	The security status of all devices on the network should be verified and validated upon requests Agents on each device that monitor end maintain the device's security Automatic patches of the security mechanisms that protect the devices Automated corrective actions that enforce the security patch	Lancope NAC



Data classification

"As Is" Now	"To Be" Target	Results Jericho Research	Possible Technologies
There are no real solutions implemented nowadays for corporate data Data mining and neural networks applications for data classification. They do not scale and do not meet the requirements of a corporate environment The owner of a data file decides what classification level receives the file	Multi-level security Information lifecycle management (ILM) Digital rights management (DRM) Automated corrective actions that enforce the rights and privileges to certain data	Automatic and dynamic classification of all types of data on the network Multi-level security model Security Attributes assigned to data DRM ILM Segregation of duties	Kazeon solution DRM, Multi-security models Security Attributes assigned to data

End-to-end encryption

"As Is" Now	"To Be" Target	Results Jericho Research	Possible Technologies
Encryption of all the transferred data (no sensitivity levels) or no encryption at all (exposure to loss or disclosure of data) No user awareness	Sensitive data in transit has to be encrypted according to the attached security levels Authentication of the entities that communicate; secure connection establishment; Authenticated end-to-end encryption The cryptographic algorithms and primitives chosen should have not been yet broken and should provide strong protection (confidentiality, integrity). Security policies that specify the use of cryptographic algorithms and protocols for different levels of protection for data in transit User awareness regarding the protection of the data	Authenticated Encryption solutions (authentication of the entities prior to start communication; secure connection established; adequate cryptographic protocols and algorithms in accordance with the security (sensitivity) level assigned to data)	SSL/TLS IPsec XML encryption

Trust broker services

Possible Technologies	Results Jericho Research	"To Be" Target	"As Is" Now
Link contracts OpenID MS Cardspace	Trust between entities is created by four information sets: 1. Identity, e.g. authentication 2. Reputation, e.g. past behaviour of the entity 3. Behaviour, e.g. current behaviour of the user, status information about the endpoint 4. Enforcement, e.g. contracts or agreements Trusted time stamps, in order to verify the date of trusted documents (to prevent fraud) Digital signatures, recognized by law as a valid instrument for signing documents and transactions Segregation of duties	User-centric approach for authentication Creation of Trust Context Report, based on security attributes Modules able to produce standard output as security attributes, in order to generate a Trust Context Report Distributive Reputation system, in order to check reliability and skills of an entity Generated contracts based on templates and digitally sign these documents Contract and general behaviour monitoring Discovery service, will decide based on a Trust Context Report which service is best suitable for this entity. Multiple policy levels, is necessary in order to support the authorization process of different companies.	Most standard modules and services of Trust Broker Framework exist today separately, but not in a trusted environment. Service Oriented Architecture (SOA) is the best manner to provide multiple services across several companies because of the loosely coupled interactions between services. However it lacks the creation of a trusted environment

Table 3: Description of the modules of Jericho Project and possible solutions

Key Requirements for Jericho Security Architecture

- The use of open standards and protocols that are universally agreed, supported, proven, and interoperable
- High levels of integration and interoperability of the security processes and services
- Re-engineering of the security process in order to reflect the business and technological needs
- Security is applied in layers and focuses on the assets that matter most
- Well defined and complete security policies, procedures
- Extend the awareness of security based on Jericho principles at all levels in the organization; the creation of a Jericho security-based culture in the adopting organizations
- Security governance has to be implemented in organizations that adhere to Jericho principle

Benefits of a new security architecture

- Jericho security architecture enables a broad range of gains in terms of flexibility, process optimization, adequate protection for the key applications and systems, for the sensitive data in an organization's network, decreased losses due to security attacks, building trust models among business partners (entities)
- Increased efficiency of the business processes – things get done faster – that leads to a competitive advantage
- Less vulnerabilities in Jericho security architecture
- Jericho security architecture enables the creation of trust based business partnerships and collaborations among organizations, new business opportunities.
- Organizations will use public networks for collaborations and interactions within and between organizations. Basically the network will be the Internet in Jericho security architecture. This leads to cost savings for the organizations in the new electronic commerce business models.
- Synergies between companies

Challenges in implementing & adopting Jericho Security Architecture

- Development and acceptability of open standards and protocols
- The changing technologies and the interoperability
- Increasing number of electronic transactions and interactions between services
- Duplication of data and of services on the network; dynamic changes of data
- Quality and management of services
- Reduction of the complexity and of the (administration) costs

De-perimeterization: Roadmap for security

Phase 0: Project Initiation

In this phase, the organizational context, the business and technological drivers will be analyzed. Moreover, the constraints, scope, assumptions and principles for the Jericho security architecture in a federated environment will be defined.
The deliverables of this phase are:

- The Business Case for architecture, including the business and technological principles, goals, drivers and requirements
- The business models and processes underpinning the functioning of the organization
- The Statement of Architecture Work containing the scope and constraints and the plan for architectural work
- The Architecture Principles

Phase 1: Analysis & Risk Assessment - Present security status of the corporate network

Further, in this phase we will analyze the current Security and IT governance situation in the organization from different points of view e.g. business, data, applications and technology. A baseline description of the present security position, the business needs and requirements will be completed. Also, an assessment of the security infrastructure in the organization will be executed. Further, the threats and risks surrounding the critical assets of the organization and the corporate network are determined.

Analysis and evaluation of:

- Business
    - Identify the business models used by the respective organization
    - Identify the business processes
    - Identify the business needs
    - Identify the critical assets for the business (e.g. data, applications, resources etc.)
- Information Systems
    - Identify the data models; the protection & control of the data; the access to the data; the value of the data for the business
    - Identify the applications and their functionalities; the protection mechanisms for applications
    - Identify the critical applications, services of the organization

- Technology
    - Assess the security infrastructure in the organization
    - Identify the current security standards, protocols, technologies, and security services in the organization
    - Identify the threats and the risks with respect to the critical assets determined in the previous steps and for the corporate network
    - Risk Assessment & Auditing/Evaluation of the present situation
        - Users (AAA)
        - Devices
        - Data
        - TB services
        - Security policy
        - Standards
        - Threats
        - Security services
- Results of Analysis Phase
    - The security context and state of the organization
    - A risk profile of the organization
    - The risk assessment report(s)
    - The security status of the critical assets (e.g. services, applications, data) of the corporate network and the impact analysis
    - The business models and processes underpinning the functioning of the organization

Phase 2: Design of target Jericho Security Architecture

In this phase, a customized target Jericho Security Architecture will be designed in alignment with the business needs and requirements of the organization. The output of this phase will be the future security solution for the organization, represented by the target Jericho Security Architecture focused on the critical assets of the corporate network. Also, in this phase there will be defined the target process schema for the customized Jericho based network, the new or improved security policy or for the organization, and the IT Governance.

The outputs of this phase are:

- The target Jericho Security Architecture
- The target process schema for the customized Jericho based network
- The new or improved security policy
- New or improved IT Governance for the company

Phase 3: Gap Analysis

Furthermore, a Gap Analysis will be performed for the Analysis & Risk Assessment Phase and the target Jericho Security Architecture. An Impact Analysis and a re-evaluation of the security needs and requirements of the organization for migrating to a de-perimeterized network will be executed as well. We will identify as well the benefits of adopting the Jericho Security Architecture.

The outputs of this phase are:

- Gap Analysis results
- Impact Analysis
- Updated business, security and technical requirements

Phase 4: Selection of the standards, technologies

Based on the security needs, functional and non-functional requirements for the corporate network identified in the previous phases, the Jericho technologies matrix will be customized with adequate open standards and products for migrating to a Jericho based network. Essentially, the open standards and technological products will be selected for every process/module comprised in the target Jericho Security Architecture designed for the organization.

The outputs of this phase are:

- The customized technology matrix for migrating to a Jericho based network

Phase 5: Migration planning

The following actions will be executed:

- Estimation of the requirements for migration and the availability of resources
- Cost/benefit analysis of adopting the target Jericho Security Architecture
- Estimation of the migration, training and other costs
- A complete analysis of the benefits of migrating to the target Jericho Security Architecture
- The milestones and the planning for implementation per process/module are also defined