Mediate
Patient Friendly Medical Intervention

DELIVERABLE
D2.1.1 – Security and privacy requirements

Project number:	ITEA 09039
Document version no.:	1.0
Edited by:	Carlos Cavero (Atos Origin) - 2011-04-30
Reviewed by:	Keith Baker (Philips Research) – 2011-04-27

ITEA Roadmap domains:
Major: Group

ITEA Roadmap categories:
Major: Content & knowledge
Minor: Interaction

HISTORY

Document version #	Date	Remarks
V0.1	2011-03-18	Starting version, template
V0.2	2011-03-19	Definition of ToC
V0.3	2011-04-07	Draft version, contributions by partners
V0.4	2011-04-12	Updated draft
V0.5	2011-04-15	Final draft to sign of by PMT members
V0.6	2011-04-22	Review version sent to the deliverable responsible
		All “draft” versions to be deleted in the “final” version
V1.0	2011-04-30	Final Version (Approved by PMT)

Deliverable review procedure:

- **2 weeks before due date**: deliverable owner sends deliverable –approved by WP leader– to Project Manager (PM, Herman Stegehuis).
- **Upfront** PM assigns a co-reviewer from the PMT group to cross check the deliverable
- **1 week before due date**: co-reviewer provides input to deliverable owner
- **Due date:** deliverable owner sends the final version of the deliverable to PM and co-reviewer

TABLE OF CONTENTS

1 Introduction

1.1 Overview of the MEDIATE project

The objective of the MEDIATE project is to increase productivity and effectiveness in healthcare and reduce patient risk and discomfort by supporting healthcare professionals in the transition from invasive, open surgery to minimally invasive, **Image Guided Intervention and Treatment** (IGIT). By empowering the healthcare professional through more advanced technologies during the whole treatment cycle, IGIT helps them to obtain a better clinical outcome of the treatment, predictable procedure times, fewer complications, better service to the patient and lower morbidity and mortality rates.

The final outcome of the MEDIATE project are clinical demonstrators for different disease areas (cardiology, oncology and orthopaedics) that will incorporate advanced technologies in image generation & analysis, procedural navigation & guidance, decision support systems and workflow management. [1]

1.2 Purpose, Context and Scope of this Deliverable

This section discusses the main intention of the deliverable. It shows on which work this deliverable is dependent, respectively, which work will be based on it. Moreover, it outlines the target audience and the scope of this deliverable.

1.2.1 Background and Context

Practically all partners participated in order to specify the MEDIATE scenarios with partners and invited experts and stimulate the discussions regarding common security criteria to provide a private, secure and trusted healthcare environment.

The security requirements are closely related with WP2- “System Architecture”, because the robustness of the platform clearly depends on the restrictions it has. The D2.1.1 – “Security and privacy requirements” will study in depth the security requisites elicited in order to take into account the security issues in the architecture design.

1.2.2 Target Audience

The target audience of the deliverable are primarily technically partners, but also ethical, legal and sociological aspects have to be incorporated into the security model for MEDIATE. Especially, questions concerning data privacy, data security or data availability must be addressed.

1.2.3 Purpose

D2.1.1 elicits the technical security requirements for the MEDIATE architecture, based on the functional requirements derived in the use cases. Thus, it is an important foundation for a secure and robust architecture.

1.2.4 Scope

The scope of D2.1.1 is not restricted to the gathering of technical requirements, but also covers the correlation with the legal issues, because privacy and trust requirements are also important for the users.

2 Executive summary

The objective of the WP2 – “System Architecture” is to define the system architecture, the development and integration of the components, and the final validation of the system designed. As we are working in a multi-vendor situation, standards (e.g. DICOM, HL7, IHE) and international organization advises (e.g. IHE, Continua) will have taken into account. Aspects related to the security and privacy will be deeply studied and applied to the system developed. The architecture should provide interfaces for minimally invasive interventions by providing the right interface definitions for the operator, and control and data interfaces for software components in multi-modal minimally invasive systems [1].

It will furthermore define the security requirements in terms of data privacy, authentication and authorization, and message confidentiality. Moreover, the adoption of the appropriate security protocols is part of this task. For this reason, a thorough investigation in the latest security technologies will be conducted. Finally, the appropriate security strategy according to security requirements and adopted technologies will be defined and the security infrastructure will be developed [1].

This deliverable D2.1.1 – “Security and privacy requirements” aims to elicit the needed requisites to specify common security criteria, metrics, models, protocols and negotiations and conclude the security requirements for the MEDIATE scenarios in such a way as to provide a private and secure healthcare environment for the hospitals and healthcare clinics. This version is the result of the discussions regarding Security Framework maintained with clinical and technological experts in order to reach a common understanding on what security means inside the MEDIATE project.

Application security must be considered a part of overall application design. When designing application security protections, enterprises should consider several requirements such as risk associated with using information technology, the security dimensions (Authenticity, Privacy, Usability, Confidentiality …) which affect the requirements. Security and safety of the proposed services will be studied and necessary solutions to minimize risks and preserve privacy will be implemented. Legal framework for patient safety and liability as well as privacy and ethical concerns will be analyzed and an outline of a policy framework will be defined. Moreover, impacts on health care organizations and structures will be analyzed and health-economics and business models will be developed.

The identification of the assets to protect the overall platform as well as the actors is crucial for evaluating the threats and vulnerabilities of the system. The specification of the roles has been done in line with the MEDIATE scenarios which will cover the functionalities and expectations of the framework. The Security dimensions are described taking into account the different components of the MEDIATE platform. A textural treatment/summary of the requirements is essential to easily understand the purpose of the document. Implications of standardization activities are also listed in order to integrate the MEDIATE system with the major european and national initiatives.

3 Security Requirements Engineering

3.1 Introduction

In principle, every software or application development project must be clearly defined before development begins. It must address a problem that the organization currently has. A requirement is a condition or capability that must be met or possessed by a system or system component to satisfy a contract, standard, specification, or other formally imposed documents. The Requirements Management (RM) and gathering process is a necessary step in order to come up with a solution appropriate for the organization. The work mostly done in this phase is performed by a person or team referred to as a requirements analyst. Requirements management involves establishing and maintaining an agreement with the customer on the requirements for the software project. The agreement forms the basis for estimating, planning, performing, and tracking the software project's activities throughout the project lifecycle. The primary activities within requirements management include:

- Planning the requirements phase
- Establishing the requirements process
- Monitoring and controlling requirements changes
- Tracking progress
- Resolving issues
- Verification and validation process

A requirement is categorized as "functional" if it specifies what the system needs to do. Otherwise, it is categorized as "non-functional." Apart from the above attribute it is important to attach further attributes to the Requirements Management process in order to provide data for continuous improvement, especially around the data used to support the estimating process. Focus should be paid to measures that provide an insight into the effectiveness of the process. The most important attributes between others could include:

- *Requirement status*, it consists of different values which define the status of each requirement in the process.
- *Requirement type*, if the requirement is functional or non-functional as mentioned above.
- *Requirements priority,* this metric provides a priority to our requirement in order to evaluate for example the effort and the prioritization of each one. Blocker, Critical, Major, Minor and Trivial are indicative.
- *Requirements traceability* is another aspect that refers to the "ability to follow the life of a requirement, in both forwards and backwards direction, i.e. from its origins, through its development and specification, to its subsequent deployment and use, and through periods of ongoing refinement and iteration in any of these phases. This ability is an essential feature in the requirements management process.

The key to requirements management is communication as well. A good requirements management process helps ensure a high level of communication between stakeholders. For the developers to fully understand the needs of the customers, they

must fully understand those needs, and have an open channel of communication among them.

Communication is also crucial when requirements change, as they do in any project. Once changes have been agreed upon, they must be incorporated into the project scope, and be communicated to developers and customers, as well. An effective means of communication is thus essential to getting the project right the first time and avoiding expensive re-work later in the development cycle.

The final implementation of an OR for IGIT, is by force of necessity a evolutionary entity. An Entity, which must be flexible and can accommodate to the needs of the patients and staff. This makes design of the MEDIATE platform a challenge in terms of architecture.

3.2 Questionnaires and Architectural Issues List

3.2.1 Introduction

As described in the Full Project Proposal (FPP) [1] the *WP2 System Architecture* delivers in M9 the *Technical report focusing on the use cases*. The use cases (or end user scenarios) will be delivered in M6 by *WP1 End-user and functional requirements* [13].

For this deliverable, it is needed to take into account the choices made in order to design a robust architecture but focusing in the MEDIATE use cases. The security framework will apply the corresponding countermeasures to protect this information.

3.2.2 Goal

For creating the *Technical report focusing on the use cases* information from different WPs is needed. This information shall be related to the use cases. The goal of this questionnaire is to obtain the information from the use cases in order to create an open reference architecture that supports the components of the rest of the WPs. We also need an open and scalable model because data exchanged will be coming from heterogeneous components. The inherent complexity of MEDIATE project concept will add intricacy to the final architecture in**:**

- Platform independent interoperability
- Loose coupling between components
- Workflow management
- Support to three different domains
- Standard compliance
- **Enhanced security adds more complexity**

3.2.3 Context

The *WP2 System Architecture* will focus on the infrastructural needs for the different WPs (1, 3, 4, 5 & 6); it will not focus on the internal design. Therefore, each WP will be seen as a black box, see figure 1 [13].

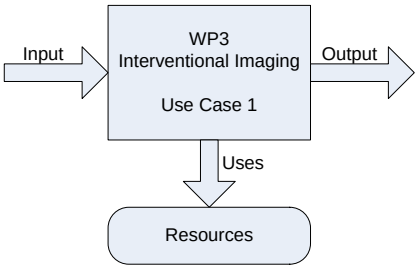

Figure 1 Black box approach

Each black box has inputs, outputs and it uses resources. The questionnaire will focus on the characteristics of these three aspects. For each use case, the WPs can have different needs. Therefore, the questionnaire shall be answered per use case.

Each WP will focus on a different time domain:

- Real time/low latency — WP 3 Interventional imaging
- On-line domain — WP4 Navigation & steering of instruments
- Off-line domain — WP5 analysis, decision support & information management

The WP6 will provide a transversal point of view of all UI designed within MEDIATE project, thus affecting real time, online and offline domains at a time.

Questionnaire

ID	Question
Inputs	
1.1	What inputs are needed?
1.2	What are the characteristics of these inputs?
1.2a	Type of the input (e.g. video, data, user interface etc)
1.2b	Format of the input (e.g. DICOM, streaming media, etc)
1.2c	Performance/Latency/Size of the input (e.g. absolute size, MB/sec, etc)
1.2d	Quality of the input (e.g. is the input critical for the application)
Outputs	
2.1	What outputs are needed?
2.2	What are the characteristics of these outputs?
2.2a	Type of the outputs (e.g. video, data etc)
2.2b	Format of the outputs (e.g. DICOM, streaming media, etc)
2.2c	Performance/Latency/Size of the outputs (e.g. absolute size, MB/sec, etc)
2.2d	Quality of the input (e.g. is the input critical for the application)
2.3	Should the output be stored? What kind of information should be stored (e.g. video, images, data, etc) and what characteristics (e.g. format, size, etc)?
2.4	Are there specific needs for display of video/data? (e.g. latency)
Resources	
3.1	Are there specific needs for (computer) resources (for example CPU/GPU power and/or memory)?

4 MEDIATE Use Cases

4.1 General overview

The use cases have been described taking into account the three types of clinical intervention scenarios: cardiovascular, oncological and orthopaedic applications. The use cases cover patient care episodes and periods related to the diseases addressed in the technology development work packages. Each use case introduces the clinical background, followed by a schematic description of the clinical scenario. In addition, two generic technology use cases are described that interface with the clinical scenarios. Each use case was drafted in close collaboration with clinical end users [14].

4.2 Use Cases Analysis

In the following sections we will enumerate the use cases identified in MEDIATE project [14], which served as the basis of the requirements elicitation. The evaluation of the possible scenarios will allow us considering all the components of the system and protecting each element accordingly.

4.2.1.1 Use case 1: RF ablation of cardiac arrhythmias

High-level goals: • Cure patient suffering from atrial fibrillation (AF) or ventricular tachycardia (VT) • Localize ablation target region AF: Find origin of pulmonary veins in left atrium VT: Find entry/exit site of the known clinical VT • Terminate the arrhythmia by RF ablation • Verify success of intervention • VT: Evaluate potentially present additional (non-clinical) VT's
Involved personnel (Actors) • Radiologist / cardiologist (pre-op imaging) • Electrophysiology doctor (EP-doc) • Supporting personnel (nurse)
Environment • MR/CT scanner for 3D pre-operative imaging • Catheterization laboratory • Sterile environment • Protection needed for X-ray radiation (lead skirt, lead screens) • Multiple monitors (many) to display various signals: ECG, signals blood pressure, blood oxygenation, etc and to display various images (X-ray, CT, MRI, 3D Elecro-anatomical map, Ultrasound)

4.2.1.2 Use case 2: Transcatheter Aortic Valve Implantation

High-level goals:

• Cure patient suffering from aortic stenosis • Determine the puncture site and intra-operative observation pose • Find and track the path from the femoral artery to the deployment site, passing through the native valve • Position the endovascular device to deploy the valve prosthesis • Verify success of intervention
Involved personnel (Actors) • Radiologist / cardiologist (pre-op imaging) • anesthetist • TAVI docs : Interventional cardiologist, surgeon • Supporting personnel (nurse)
Environment • CT scanner for 3D/4D pre-operative imaging, US imaging • Catheterization laboratory, or operating / hybrid room • Protection needed for X-ray radiation • Multiple monitors to display various signals and images

4.2.1.3 Use case 3: Percutaneous Coronary Interventions

High-level goals: • Myocardial revascularization of patients suffering from anginal symptoms • Pre-operative: find hemodynamically significant coronary lesion • During intervention: a. Cross (in case of total occlusion also open) and dilate the lesion b. Stent lesion c. Verify success of intervention
Involved personnel (Actors) • Radiologist/ cardiologist (pre-op imaging) • Interventional cardiologist (IC) • Supporting personnel (nurse)
Environment • Pre-operative (diagnosis): X-ray angiography, and/or MR perfusion / CT angiography • Catheterization laboratory • Sterile environment • Protection needed for X-ray radiation (lead skirt, lead screens) • Multiple monitors (many) to display various signals such as ECG and interventional images (X-ray) • Interventional devices: a. Guide catheter b. Balloon catheter c. Balloon-mounted stent d. Guide wires

4.2.2 Oncological image guided interventions

4.2.2.1 Use case 4: Needle ablation of tumors

High-level goals: • Efficient and effective identification of tumor location and type • Planning of minimally invasive tumor treatment • Dose reduction for interventional radiologist and patient • Outcome control of tumor treatment
Involved personnel (Actors) • Radiologist (pre-op and/or post-op imaging) • Interventional Radiologist (treatment) • Supporting personnel (tech, nurse) • Radiation oncologist • Urologist • Clinical physicist • Radiation technologists • Robot technologist • MRI physicist
Environment • MR/CT scanner for 3D pre-operative imaging • Interventional radiology Suite • Protection needed for X-ray radiation (lead skirt, lead screens) • Checks and controls for MR Conditional implants • Brachytherapy equipement • Ablation catheter equipement (cryo, RFA, microwave) • Biopsy needles

4.2.2.2 Use case 5: Tumor treatment: MR-guided HIFU

High-level goals: • Cure patient suffering from uterus myoma (UM) • Determine maximum volume for ablation by hifu • Ablate the myoma • Verify success of intervention (post-op and long-term follow-up)
Involved personnel (Actors) • Radiologist (pre-op imaging) • Intervention radiologist • Supporting personnel
Environment • MR scanner for 3D pre-operative imaging • MR-Hifu scanner

4.2.3 Orthopaedic interventions

4.2.3.1 Use case 6: Bone tumor navigation

4.2.3.1.1 Use-case 6a: bone tumor resection

1	**High-Level goals:** ▪ Cure patient suffering from bone tumor ▪ Perform the reconstruction of the resected bones ▪ Verify success of intervention
2	**Involved personnel (Actors):** ▪ Radiologist ▪ Surgeon ▪ Nurses
3	**Environment:** ▪ MR/CT scanner for 3D pre-operative imaging ▪ US imaging devices for intraoperative registration ▪ Sterile environment ▪ 3D localizers ▪ Protection required for x-ray radiation

4.2.3.1.2 Use Case6b: metastases and benign tumors

1	**High-Level goals:** ▪ Cure patient suffering from a benign tumor or a bone metastasis
2	**Involved personnel (Actors):** ▪ Interventional radiologist ▪ Nurses
3	**Environment:** ▪ MR/CT scanner for 3D pre-operative imaging ▪ US imaging devices for intraoperative registration ▪ Sterile environment ▪ 3D localizers ▪ Protection required for x-ray radiation

4.2.3.2 Use case 7: Corrective osteotomy

High-level goals: • Cure of patients suffering from malunion of bone fragments • Restoration of the correct relative poses of bone fragments • Planning of the desired end poses of bone fragments • Navigation of bone parts • Verification of the success of intervention intra-operatively • Comparison of planning with post-operative situation
Involved personnel (Actors) • Radiologist / surgeon (pre-op imaging) • Physicist / surgeon (pre-op planning & intra-operative navigation)

• Supporting personnel (nurse)
Environment • CT scanner for 3D pre-operative imaging • Operation room • Sterile environment including sterile coverage of new instruments. • 3D per-operative imaging • Protection needed for X-ray radiation (lead skirt, lead screens) • PC and software for pre-operative planning and to support per-operative navigation. • Mechanical devices for controlled positioning of bone parts

4.2.4 Generic technologies for minimally invasive intervention support

4.2.4.1 Use-case 8: Innovative user interfaces in minimally invasive treatment

Several limitation exist in the current UI and GUI designs –

- Inadequate system design with respect to the target environment;
- Inadequate GUI design;
- UI not suited for optimal workflows, thus causing unnecessary interruptions;
- Significant learning curves for each individual system.

In our work, we will therefore make sure to take into account the known constraints, fundamental to any UI design, such as, but not limited to,

- Environment related constraints such as for instance sterility constraints, physical constraints of the operating room such as space and acoustics, …
- Task related constraints such as direct user control over surgical tools and equipment, minimal learning curve, minimal if any impact on user workload, …

A next step of further development could be the introduction of Clinical Decision Support (CDS) systems. CDS systems are typically designed to aid decision making for prevention, screening, diagnosis, treatment, drug dosing, test ordering, and/or chronic disease management, and “push” the information to the decision maker.

In basic terms, these models are based on a health care system, which includes the clinician nested in a work system nested in a health care organization, determining the physical, cognitive, and socio-behavioral performance of the clinician. The clinician’s performance subsequently helps to determine outputs such as patient safety and health care quality. CDS automation must be designed to meet clinician performance needs such as sensation, perception, searching, memory, attention, decision making and problem solving. If the design of the CDS is poor, then clinician performance suffers. If clinician performance suffers, patient care suffers.

CDS however goes much further than a “simple” user centered design but could definitely roll out as the next big wave in healthcare IT. It is, unfortunately, outside the scope of this project.

4.2.4.2 Use case 9: Single Incision Laparoscopic Surgery (SILS) for partial nephrectomy

1	**High-level goals:** • Cure patient suffering from renal tumors • Check tumor • Proceed to ablation • Verify success of intervention
2	**Involved personnel (Actors)** • Clinical examination • Radiologist and oncologist (pre-op: CT scan +/- Ultrasound) • Nurse and labs (pre-op: blood test) • Laparoscopic surgeon (if surgery is indicated after cancer extension check) • Pathologist (during or after op: cancer confirmation) • Supporting personnel (nurse)
3	**Environment** • CT scan +/- Ultrasound machine for pre-operative imaging • Sterile environment • Per-operative Ultrasound to locate tumor • Multiple monitors to display various signals: ECG, signals blood pressure, blood oxygenation,… and to display various images (CT scan, Ultrasound) • Robotized laparoscopic tools: endoscope holder, hand held motorized articulated surgical instrument (grasping, retracting, mobilizing, dissecting and suturing)

4.3 Security dimensions

We can characterize security in terms of key security concepts [ISO/IEC 27002]: confidentiality, integrity, authentication, authorization, non-repudiation, and availability. These security goals are never absolute: it is not possible to guarantee 100% confidentiality, non-repudiation, etc. However, a well designed and implemented security response model can ensure acceptable levels of security risk. For example, using a well-designed cipher to encrypt messages may make the cost of breaking communications so great and so lengthy that the information obtained is valueless.

While confidentiality and integrity can be viewed as primarily the concerns of the direct participants in an interaction; authentication, authorization, and non-repudiation imply the participants are acting within a broader social structure [2].

4.3.1 AAA (Authentication, Authorisation and Accounting)

Authentication concerns the identity of the participants in an exchange. Authentication refers to the means by which one participant can be assured of the identity of other participants.

Authorization concerns the legitimacy of the interaction. Authorization refers to the means by which an owner of a resource may be assured that the information and actions that are exchanged are either explicitly or implicitly approved.

Accounting is the capability associated with resources that allows for the use of those resources to be measured and accounted for. This implies that not only can the use of resources be properly measured, but also that those using those resources also be properly identified.

Authentication, Authorization, and Accounting (AAA) is a term for a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. These combined processes are considered important for effective network management and security [10].

4.3.2 Availability

Availability concerns the ability of systems to use and offer the services for which they were designed. One of the threats against availability is the so-called denial of service attack in which attackers attempt to prevent legitimate access to the system.

We differentiate here between general availability – which includes aspects such as systems reliability – and availability as a security concept where we need to respond to active threats to the system.

4.3.3 Confidentiality

Confidentiality concerns the protection of privacy of participants in their interactions. Confidentiality refers to the assurance that unauthorized entities are not able to read messages or parts of messages that are transmitted [5].

Note that confidentiality has degrees: in a completely confidential exchange, third parties would not even be aware that a confidential exchange has occurred. In a partially confidential exchange, the identities of the participants may be known but the content of the exchange obscured.

4.3.4 Integrity

Integrity concerns the protection of information that is exchanged – either from unauthorized writing or inadvertent corruption. Integrity refers to the assurance that information that has been exchanged has not been altered.

Integrity is different from confidentiality in that messages that are sent from one participant to another may be obscured to a third party, but the third party may still be able to introduce his own content into the exchange without the knowledge of the participants.

4.3.5 Non-repudiation

Non-repudiation concerns the accountability of participants. To foster trust in the performance of a system used to conduct shared activities it is important that the participants are not able to later deny their actions: to repudiate them. Non-repudiation refers to the means by which a participant may not, at a later time, successfully deny having participated in the interaction or having performed the actions as reported by other participants.

4.3.6 Privacy

The term "**privacy**" is used frequently in ordinary language as well as in philosophical, political, legal and of course in Information Technology discussions, yet there is no single definition or analysis or meaning of the term. The concept of privacy has broad historical roots in sociological and anthropological discussions about how extensively it is valued and preserved. Moreover, the concept has historical origins in well known philosophical discussions, most notably Aristotle's distinction between the public sphere of political activity and the private sphere associated with family and domestic life. Yet historical use of the term is not uniform, and there remains confusion over the meaning, value and scope of the concept of privacy.

Privacy is not about data—it's about people. Privacy is not secrecy, and it is not about hiding information. Privacy is concerned with the proper handling of personal information and with respecting the dignity of the individual to whom the information refers. The fundamentally contextual nature of the use of personal information prevents us from formulating a single strict definition of "privacy." However, privacy principles accommodate this contextuality and guide the development of enterprise privacy practices that can reduce risk and cost [4].

In health care, working with anonymity or pseudonymity is an established standard, e.g., in medical studies. However, for MEDIATE's use cases, anonymity does not seem to be an option because the MEDIATE platform purpose is to connect users to EPR/HER systems, provide HPs or patients with access to an EPR/HER system located at a clinic or a GP's surgery, respectively. Thus, both ends need a trait to relate to each other. Nevertheless, they do not necessarily have to disclose their real-world identities to the platform. For the services provided by the platform, it will normally not matter whether the patient is known by her real name or by some artificial trait. Hence offering pseudonymity is an option for the platform. It may not make sense for the patient to be against the MEDIATE platform, and the same goes for HPs. This should not be taken as general distrust against the platform but as an additional safeguard against security/privacy breaches, like hacker attacks. Regarding clinical information patient privacy should be assured which means that no personal data will be stored in the system, and the identification must be through id or numerical series preserving the individual disclosure. The platform will not allow any personal identification by means of radiological images, so no private data will be included inside the DICOM files.

5 Security Requirements: MEDIATE Platform

The term **requirement** "in engineering, it is a singular **documented need** of what a particular product or service should be or perform. It is most commonly used in a formal sense in systems engineering, software engineering, or enterprise engineering. It is a statement that identifies a necessary attribute, capability, characteristic, or quality of a system in order for it to have value and utility to a user.

In the classical engineering approach, sets of requirements are used as inputs into the design stages of product development. Requirements are also an important input into the verification process, since tests should trace back to specific requirements. Requirements show what elements and functions are necessary for the particular project."

Requirements Classification: from Wikipedia requirements are typically placed into these categories:

- Functional requirements describe the functionality that the system is to execute; for example, formatting some text or modulating a signal. They are sometimes known as capabilities. (F)
- Non-functional requirements describe characteristics of the system that the user cannot affect or (immediately) perceive. Nonfunctional requirements are sometimes known as quality requirements or ilities. (NF)
- Constraint requirements impose limits upon the design alternatives or project/process operations. No matter how the problem is solved the constraint requirements must be adhered to. (C)

The security requirements for the MEDIATE platform have been divided into several categories taking into account protection, privacy and security issues of the MEDIATE platform: General, Data Message, Communication, Access Control, Digital Entities and Privacy.

5.1.1 General

The overall purpose of the security framework is to protect the system from the attacks outside the platform, but also to avoid the misuse of the available critical and personal information. At this stage the first important requisite is the Platform Integrity for the stored data in order to guarantee the integrity of the stored data in the case of an unwanted happening. Security and privacy related to patient data are of utmost importance. The patient data should be transfer and maintained in a secure way while any access to them should be monitored and logged (getting advantage of a login mechanism available in the applications). Of course, in MEDIATE, we are dealing with sensitive data, thus security must be available on all platforms. Scalability, Modularity and Transparency will facilitate the implementation of the protection mechanisms, because at the end, security must not materially impact the performance of the system.

As it is mentioned before, security deals with protection, not only protection against loss or replication of data transferred between two systems but also protection against threats and against unintended user actions. Because of the short of data (medical) stored in the system, the unwanted access to the information should be avoided. Therefore unauthorized persons should not obtain administer rights through the

internet and not access to personal data. The system must conform to US Law on Handling Personal Data. The data integrity and the overall functioning of the platform must be assured in order not allowing the system to close down, neither on the client nor on the server. All data entered must be checked for format, consistency and validity. In case of doubt, the user must be warned and asked what to do.

MEDIATE architecture must provide **assurance** that it delivers the security and compliance properties it promises. The obligations to comply with the security regulations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which require "the system, its health care components and users in order to protect the **confidentiality**, **integrity** and **availability** of individually **identifiable** (not necessarily personal) health information created, received, transmitted or maintained include the implementation of security measures and particular safeguards to ensure the abovementioned issues, the protection against any reasonable anticipated threats and uses or disclosures of personal data which are not permitted under the federal laws".

In such a way the triple A, **Authentication**, **Authorisation** and **Accounting** [10] should assess:

- The data's quality, incorporating mechanisms to verify that for instance the blood glucose measurements or personal data is originated from a known/trusted source.
- The relevant actions should be made by the correct person, thus it should be clear who made the decision, what kind of decision was made and when it was made.

5.1.2 Data/message Security

The security framework aims at ensuring the information in the system. The data/message transmitted between the different components in MEDIATE platform and clients must be protected. In the MEDIATE system it will be necessary to ensure the data/messages exchanged between the components and MEDIATE platform by means of message authentication. The security of messages transferred between them must be ensured even after the message was received and should be assure even if the message was received over a secure communication channel. To guarantee this, the messages themselves must be self-contained with respect to authenticity, integrity, and confidentiality. Likewise the data/message exchanged between the MEDIATE server and the EPR/EHR System and the GP EPR should be authentic.

5.1.3 Communication Security

The communication security is the protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. In the MEDIATE system it will be necessary to ensure the communications between the components and the server by means of entity authentication. It must be assumed that data transmission from the different entities and vice versa takes place over an insecure channel, i.e., data might be overheard or tampered with. Since personal data is to be transmitted it must be ensured that the communication channel is authentic, with integrity, and confidential.

5.1.4 Access Control

Access control is a system which enables an authority to control access to areas and resources in a given physical facility or computer-based information system. In MEDIATE system the patient identification should be automatic in order to avoid identification mistakes. Risks of wrong patient identification have to be negligible. The MEDIATE identification system must be flexible enough to integrate existing identification methods employed on site, e.g., OR in a hospital.

Sharing patient data is necessary in health care to treat patients but access should only be given to persons involved in the treatment, for this reason access to sensitive information should only be given to authorised personnel preventing the misuse of data. Each person in the MEDIATE platform will have the right to perform a certain set of actions. In order to simplify the administration of these rights, each person will be assigned to a role and roles are assigned to permissible actions. The advantage of this approach is that it is easier to manage the rights of a role than managing individual rights for each person.

The administrator of the MEDIATE system should assign the roles to the corresponding people in order to allow the users accessing to the right set of information and actions to be done with the data.

5.1.5 Digital Entities

In the MEDIATE platform, entities must be uniquely identifiable and recognisable by digital entities in order to allow repeated communication, referrals, accountability of actions, exclusion of ill-behaving entities, etc. Digital identities for the MEDIATE platform MUST only be issued or revoked by trusted (third) parties, e.g., a Certification Authority (CA). Without a Trusted Party (TP), anyone could produce its own digital identity and someone relying on such an identity would have to trust that the claimed identity is genuine. By incorporating a TP, relying parties trust that the TP ensures that its issued digital identities are genuine. This makes life easier for relying parties as they only have to establish a single trust relationship (with the TP) as opposed to having a multitude of trust relationships with others. The same goes for parties that had been excluded from the MEDIATE platform, as each relying party would have to determine by itself if another party is still part of the MEDIATE platform or not. In case of a trusted party, the relying part could simply query the TP if some identity is still valid or had been revoked, e.g., because its owner left the platform.

5.1.6 Privacy

Privacy ensures that individuals maintain the right to control what information is collected about them, how it is used, who has used it, who maintains it, and what purpose it is used for. In such a way handling of personal data has to conform to privacy laws. In MEDIATE system in order to protect the privacy of the users personally identifiable information (PII) and further more personal data the focus will be in enhancing the privacy of the individual inside the platform. Each message in each transmission channel shall be separated from the patient data and association between measurements and patient shall not be possible for whoever can intercept the measurements. In particular, personal data shall be rendered anonymous or pseudonymous as allowed by the purpose for which they are collected and/or further processed or used. This (might be/) is in conflict with unnecessary collection of personal data, which are not required to fulfil a specific task. MEDIATE platform has to tackle these privacy issues.

The modules should provide security mechanism for data stored in the MEDIATE platform. Patients have to acknowledge that personal data gathered from them can be stored and transmitted within the technical infrastructure of MEDIATE. Therefore the patient has to sign a consent form and the information about this should be also stored inside MEDIATE repository. It should be possible to exclude several personal information from storage/transmission.

Currently all actions are recorded on a paper chart/record. Because of data privacy protection and safety issues this record must not stay at the patient's bed but will be stored centrally. The staff has to look for the patient record every time before he/she goes to the patient. This means that the information is only available for one person at the same time. Furthermore, in an information processing chain, several stakeholders might be involved but it might not be necessary for every stakeholder to know which exact data another stakeholder has processed.

The patients have to give their consent to MEDIATE system in order to use their personal information. For this reason, information related to informed consent has to be stored. An ethical approved informed consent has to be signed (either digitally or in paper form) by patients before they can be enrolled in the MEDIATE platform. The enrolment procedure shall allow the storage of the digitally signed informed consent or of a scanned copy of the paper form signed informed consent and this procedure shall be completed before any other operation can be performed. The consent must be verifiable by the MEDIATE Server. This consent must not be considered valid if the patient was not involved in the decision and it must be possible to revoke the consent. A patient must have the option to decide whether personal data is processed or not at any time. If the patient once gave her consent it must still be possible for the patient to revoke her consent, which means that any further processing of the affected data is forbidden. Also, if a patient revoked her consent the existing data may not necessarily be deleted, however, it must be excluded from any further processing.

Privacy laws require that data subjects have to consent to the transmission and processing of their data. If a new data item is to be transferred which was not foreseen in the initial consent, the subject has to give a 'new' consent before the new data item can be transferred and subsequently processed. The transmission must include some kind of notice to inform the requesting party, usually the patient's doctor, that some data item was not transmitted and that the subject should be asked for an extended consent.

6 Standardization Activities

A custom application security framework can implement an enterprise's unique security requirements that are not supported by platform or third-party frameworks. A custom framework can hide the differences between the security features of different programming languages and development platforms. And a custom framework can define security features in isolation from the underlying systems that actually implement the many aspects of security functionality.

Government regulations such as the Health Insurance Portability and Accountability Act (HIPAA), and the EU Directive 95/46/EC on Data Protection [6], as well as industry standards such as the Payment Card Industry (PCI) Data Security Standard (DSS) mandate specific levels of auditability, confidentiality, and other forms of information security. Enterprises subject to such regulations have much to lose if they cannot comply. For these organizations, developing a custom security framework that can be easily used by all applications regardless of platform or programming language is well worth the effort and expense.

Most large organizations have highly heterogeneous information technology (IT) environments. Enterprises typically rely on multiple application platforms, such as .NET, Java EE, mainframe systems, ESBs [3], and so forth. Native security frameworks are by definition specific to an application platform; their APIs and programming libraries are not portable to or usable from other platforms. Third-party frameworks are often tied to vendors' infrastructure products, and unless their APIs are completely based on open standards such as SAML, WS-Security, or XACML [7], their interoperability with other infrastructure is limited. Open source frameworks are either language-specific or limited in functionality. An enterprise should invest in developing a custom application security framework if it wants business developers to use identical techniques and APIs on all platforms.

SAML 1.1 has become the de jure and de facto standard for most federated identity activity. Additional federated identity standards are still being developed by the Shibboleth project, the Liberty Alliance, and the Web Services Federation (WS-Federation) Technical Committee at OASIS.

The Shibboleth Project, a project of Internet2, a higher education consortium, is developing architectures, policy structures, practical technologies, and an open source implementation to support inter-institutional sharing of web resources subject to access controls. The Shibboleth Protocols and Profiles specification, which builds on SAML 1.x, was submitted to OASIS [9].

The Liberty Alliance initially focused on addressing federation requirements for web application. The Liberty Identity Federation Framework (ID-FF) extends SAML 1.x to enable web-application account linking, and this specification has been submitted to OASIS. SAML 2.0, which was ratified March 2005, brings together SAML 1.x, Liberty ID-FF, and Shibboleth functionality, and supports: authentication, authorization, and attribute assertions; single logout; account linking; attribute exchange; metadata exchange; pseudonymity; and other functions into a single set of specifications.

The Liberty Alliance has also developed the Identity Web Services Framework (ID-WSF), which provides a framework for creating and interacting with identity-based services, which are web services that can retrieve information about an identity,

update information related to an identity, or perform some action for the benefit of some identity. ID-WSF includes a security framework for identity-based web services that extends WS-Security. ID-WSF also includes authentication, authorization, and SSO frameworks based on SASL that can support simple identity federation across web services using a credential mapping model. These capabilities compete, to a degree, with WS-Trust [8].

The WS-Federation specification builds on and extends the WSSF to support federation for web services. Similar to SAML 2.0, WS-Federation supports single logout, account linking, attribute exchange, metadata exchange, and pseudonymity, but unlike SAML 2.0, it provides these services for both web applications and web services. WS-Federation also supports claims-based authorization and protection of a principal's privacy with respect to claims asserted in security tokens.

Another dimension is related to the *DICOM Security mechanisms*. First of all, one should note that the DICOM standard facilitates the exchange of information. It is only part of the overall information chain. Therefore, it is also only a relatively small part of everything an institution has to do to create a secure environment. Before a person accesses an image, there are procedures and rules about the placement of the monitor. There are access control and authorization rules that are taken care of by the application level software using passwords or even biometric access controls. There is an audit and logging mechanism required that logs any data access and by whom.

When we finally have access to the information and want to retrieve it using a non-secure line, such as the Internet, is when DICOM has to worry about the security. This is a relatively easy extension; the data can just be encrypted using standard mechanisms and utilities. Electronic signatures are another aspect of DICOM security. The electronic signatures prevent someone from changing the information without the receiver noticing it.

Security is described in the DICOM standard as well as in the IHE Technical Framework [15]. Both encryption and digital signatures have been demonstrated at RSNA and the European Congress of Radiology (ECR). The demonstration software and public source code are available for implementers to try out and use.

Technologies come and go, but software applications can have a long lifetime. By providing a high-level interface that is decoupled from platform- or product-specific features and APIs, a custom security framework can also free the enterprise to retire aging technologies and incorporate newer or more secure technologies without forcing developers to learn new methods and tools, and without rewriting existing applications.

7 Conclusions

The MEDIATE platform is organized in a decentralized manner, such that personal, medical information is transmitted and shared by several parties. Therefore, it is necessary that such data is transmitted, managed, and processed in a secure, trusted, and privacy-preserving way. This means that confidentiality has to be guaranteed in order to allow the doctors to store the clinical information with confidence. It also means that authenticity of senders and recipients of medical data must be ensured.

Access to such personal data may naturally be given to authorised entities only. If this is not the case, stored patient data could be easily manipulated which could have detrimental effects on the patient's health and would erode the trust in electronic health care. Privacy laws also play a central role in the management of personal, medical data, as often the patient's consent must be sought before any data processing can take place. Consent, whether in paper or electronic form, must be given by the patient him/herself which, of course, should be verifiable. However, the lack of consent might constrain or even prohibit the treatment of a patient as it might not be possible to make a proper diagnosis due to missing or inaccessible data. Therefore technical means for detecting and informing patients and medical personnel about missing consents have to be considered as well. The requirements can be assigned to functions and components of the data management model in the following way:

- General
- Data/message security
- Communication security
- Access control
- Digital identities
- Privacy

8 Glossary

AAA	Authentication, Authorization, and Accounting
BAN	Body Area Network
DICOM	Digital Imaging and Communications in Medicine
DoW	Description of Work
DSS	Data Security Standard
EE	Enterprise Edition
EHR	Electronic Health Record
EPR	Electronic Patient Record
ESB	Enterprise Service Bus
EC	European Commission
ECR	European Congress of Radiology
EU	European Union
FPP	Full Project Proposal
HIPAA	Health Insurance Portability and Accountability Act
HIS	Health Information System
ICT	Information and Communication Technologies
ID-FF	Identity Federation Framework
ID-WSF	Identity Web Services Framework
IGIT	Image Guided Intervention and Treatment
IHE	Integrating the Healthcare Enterprise
ISO	International Organization for Standardisation
IT	Information Technology
NFC	Near Field Communication
OASIS	Organization for the Advancement of Structured Information Standards
PAN	Personal Area Network
PCI	Payment Card Industry
PoC	Point of Care
POCT	Point Of Care Technology
QoS	Quality of Service
RFID	Radio Frequency IDentification
RM	Requirements Management
RSNA	Radiological Society of North America
SAML	Security Assertion Markup Language
SASL	Simple Authentication and Security Layer
SoA	Service oriented Architecture
SOAP	Simple Object Access Protocol (XML protocol)
SOPs	Standard Operating Procedures
SSO	Single Sign On
SOX	Sarbanes-OXley
SVN	Source Versioning Number
XACML	eXtensible Access Control Mark-up Language
XML	eXtensible Markup Language
W3C	World Wide Web Consortium
WAN	Wireless Area Network
WP	Work Package
WS	Web Services
WSS	Web Service Security
WSSF	Web Service Software Factory

9 References

[1] MEDIATE Full Project Proposal, version 8.0, 10-12-2010
[2] Application Security frameworks, Joe Niski, Burton Group, 2008
[3] Enterprise Service Bus: A definition, Anne Thomas Manes, Burton Group, 2007
[4] Identity and Privacy strategies - Privacy, Ian Glazer and Bob Blakley, Burton Group, 2009
[5] Security and risk management strategies, Information Confidentiality, Trent Henry, Burton Group 2009
[6] Working Document on the processing of personal data relating health in Electronic Health Records (EHR), Article 29 – "Data Protection Working Party" of Directive 95/46/EC, 2007
[7] Web Services Security: SOAP Message Security 1.1 (WS-Security 2004), OASIS Standard Specification, 2006
[8] WS-Trust 1.3, OASIS Standard Specification, 2007
[9] Reference Architecture for Service Oriented Architecture Version 1.0, OASIS Standard Specification, 2008
[10] A context-related authorization and access control method based on RBAC: a case study from the health care domain, Marc Wilikens, Simone Feriti and Marcelo Masera.
[11] Security and Privacy issues with Health Care Information technology, Marci Meingast, Tanya Roosta and Shankar Sastry
[12] Wikipedia, http://en.wikipedia.org/wiki/
[13] Mediate-Questionnaire-Global Architecture, v0.3, Aron van Beurden
[14] D1.2.1 - End-user scenarios and requirements
[15] "IHE Radiology Technical Framework", http://www.ihe.net