4ª ed

MIM

Identity in eHealth - from the reality of physical identification to digital identification

Maria João Magalhães Pereira Campos

MESTRADO EM
INFORMÁTICA MÉDICA
2º CICLO DE ESTUDOS

Oct|2011 17 October 2011

4ª ed

MIM

Identity in eHealth - from the reality of physical identification to digital identification

Maria João Magalhães Pereira Campos

MESTRADO EM
INFORMÁTICA MÉDICA
2º CICLO DE ESTUDOS

ORIENTADORES:

Luís Filipe Antunes, PhD

Manuel Eduardo Correia, PhD

Oct|2011 17 Outubro 2011

U. FMUP U. FC

Acknowledgements

I dedicate this thesis to my daughters, **Catarina** and **Filipa Carneiro**, whose encouragement and understanding were always present. I honestly expect that this work can contribute to a better world for them. To my husband **Luis Carneiro** for his unconditional support and encouragement, without him I would never enroll in a master degree.

To my mentor and supervisors, **Dr. Manuel Eduardo Correia** and especially to **Dr. Luis Filipe Antunes** for fruitful discussions and whose expertise, understanding and support were essential in accomplishing this work.

To my **parents** help me being focused and pursue to study and achieve more knowledge in some of my passion subjects.

Abstract

Many heterogeneous and highly specialized software applications for eHealth have been implemented and deployed by diverse health organizations, such as public and private hospitals and health care centers. The rational management of these eHealth assets together with their efficient and interoperable integration represents today a major hitherto unresolved challenge for the health sector at a global level. One of the present implications is the serious interoperability issues that arise by the lack of widely accepted standards for the homogeneous integration of the diverse identity and authentication mechanisms used by the eHealth applications ecosystem. Unfortunately this has not yet been a major infrastructure concern for the eHealth context and thus constitutes a major road block for the realization of these applications full integration potential.

It is a common occurrence that only at the time when an application is put into production there is an awareness about the sudden difficulty of integrating and conciliating the new application identity management and users profiles with what has already been done for the rest of the applications currently in production at the site. This situation is aggravated when the application leaves the local domain to be deployed at the regional or even national level, where, without a well-planned digital identification infrastructure, the applications integration difficulties can be orders of magnitude more severe.

In this work we propose a new high level model for the secure identity provisioning of eHealth applications. The critical infrastructure standard components required for such an infrastructure, together with the Portuguese eID smart-card, allow us to delineate a novel and highly flexible infrastructure for secure identity management and authentication services for eHealth.

The secure privacy oriented identity infrastructure we propose fits well within the specific needs of highly diverse eHealth applications, precisely because it provides a strong foundation, upon which more reliable, secure, trustworthy and real interoperable eHealth applications can be built and deployed.

Thesis Structure

The structure of this thesis is as follows:

Chapter 1 introduces the main background knowledge needed for this research. We discuss the main significance and problems regarding identity and authentication in the eHealth context. We provide definitions on eHealth and identity management, assess the most relevant national and European legislation and summarize the goals and the main contributions obtained by our research work.

Chapter 2 presents a comprehensive technical review of recent research that is relevant to the subject of this thesis. It covers the topics of identification, authentication and authorization mechanisms in the context of identity management in eHealth. It further provides a description of the main issues involved and presents future perspectives on identity management in eHealth as well as the main results of the most relevant themes identified in the literature.

Chapter 3 presents the current state of the art on identity management systems and standards. It covers the current most relevant work in practical identity management and identifies the technical requirements of a practical framework for identity management in eHealth.

Chapter 4 introduces the proposed identity management framework for eHealth. In this chapter we propose and describe in detail a new identity management provisioning model, explaining in the detail the main components required for eHealth. We justify the framework model and describe its proper use in order to maintain its trustability and reliability.

Chapter 5 presents some use case scenarios inspired by real news taken from reliable sources. These identified use case scenarios provide concrete examples of the practical applicability of the proposed identity model. We also provide a detailed risk assessment for each one of the described use case scenarios and indicate how one might mitigate the identified risks.

Chapter 6 concludes the thesis by identifying and summarizing the main contributions, recommendations and limitations. We also identify some research topics that have not been covered by this thesis, but that can constitute fruitful directions for further future work.

Scientific results

1. **Proceedings of the International Conference on Health Informatics – HEALTHINF 2011**

Maria João Campos and Pedro Pereira Rodrigues. "Key Issues and Future Perspectives on Identity Management in eHealth: A Review". In Proceedings of the International Conference on Health Informatics - HEALTHINF 2011, pages 455-458, ISBN 978-989-8425-34-8, INSTICC Press. Rome, Italy. January 2011

2. **45th IEEE International Carnahan Conference on Security Technology 2011**

Maria João Campos, Manuel E. Correia and Luís Antunes. "Leveraging identity management interoperability in eHealth". In Proceedings of the International Conference on Security Technology – 45th° IEEE International Carnahan 2011.
Barcelona, Spain. October 2011

3. Working paper with PhD Ricardo João Cruz-Correia, **"The Portuguese Health Information Backbone – Twenty years of history of SONHO and SINUS"**

Contents

1 List of Figures

2 List of Tables

1 Introduction

The software applications for the Portuguese health sector have traditionally been planned, deployed and used by different health organizations such as hospitals, public and private health care centers, without having a previously common agreed upon standard for inter-operable identity provisioning and authentication mechanisms. There are however some examples of successful initiatives that were lunched to create national identity repositories, such as the unique patient's identification [1]. Unfortunately other important and necessary identity repositories for eHealth professionals and other health related organizations are yet to be defined.

There are already examples of eHealth applications that promote patient empowerment by providing valuable and useful information on personal health data [2]. However, these applications suffer from a registration process with a high risk of identity theft since they rely on critical identity mechanisms that do not require strong authentication for service enrollment and subsequent information access and are therefore more vulnerable and prone to cyber-attacks [3].

The national citizen eID card is currently considered to be an excellent opportunity [4] to build upon and improve security for health information systems. This is being materialized by the plethora of newly planned government digital services that use the citizen card for authentication and where the digital qualification of professionals and the citizen's/patient's explicit secure consent for access to specific information attributes are assets sorely needed for their successful deployment. Unfortunately appropriate inter-operable secure mechanisms for the professional's qualified authentication and citizen's explicit consent for private information access are presently not implemented or even defined. The existing authentication model for the citizen's card is centralized into a national government managed authentication framework. In an eHealth application context the citizen's card can be correlated with the patient identification number, but the question that arises then is whether it is possible to establish an appropriate relationship of trust between the different administration contexts (Government vs. Health) to provide the necessary proof of the citizens' consent for allowing the access to highly specific critical health related information.

Finally, during our initial research we realized that there is no integral analysis of the current status of identity management for eHealth in Portugal, and consequently it is not possible to directly compare the Portuguese situation with what is currently happening in other European Countries.

To better illustrate the kind of complex issues that are being addressed by our identity management model, consider an identity scenario where a physician is allowed to auto-enroll into an electronic prescription application. The supporting identity infrastructure would have to involve several actors and would have to provide strong guarantees for the following actions and assertions (1) the person is who he says he is (2) he is a physician (3) determine the organization/position he works for, including for example the location where the application is currently being used to issue medical prescriptions. In this example the citizen's card can solve the issue of proof of the person being who he says he is, however this does not qualify him as a physician. To prove that the user is a physician, it is necessary to access the institutional entity that manages the registry of his profession and request, in a secure electronic form the proof that the user is a physician. To complete the process, it is still necessary to obtain accurate information about the prescription location and assure that the physician is allowed to access prescription functionalities at that location.

Issues related to identity management are not only structurally related to interoperability, but must also include a functional understanding of the peculiarities of eHealth activities to be reflected in the functions, responsibilities and roles acted upon different systems by different entities profiles. It is also important to ensure agreed upon inter-operable standards and procedures for identity management and authentication, fully accepted and complied upon by different entities in different domains of authentication. The criteria and policies for the quality assurance of the registration procedures that are used to determine identity and their relevant characteristics, and subsequently the management of the full identity life cycle must also be defined and fully agreed upon by all the participants.

Identity management for eHealth is also complex due to the difficulty in managing a central registry of professionals and service provider's identity that can keep up with updated identity attributes and respective life-cycles, especially if one considers the high mobility healthcare professionals can have between different health organizations. It is thus necessary and of great value to create a federated model for identity management and authentication for eHealth that takes into special consideration the cross-organizations and the healthcare professional's mobility, and at the same time promotes, for example, the development of eHealth systems that can securely provide search and access to patient medical records, located in several different hospitals or practices and at the same time cater for the patient expected privacy concerns.

1.1 Objectives and contributions

The main objectives and contributions achieved with this thesis are:

- A literature review on identity management for eHealth. Based on this we have obtained a more detailed understanding of the main issues involved and of the future perspectives we can have about this subject;
- A characterization of the state of the art in identity management, emphasizing the current existing gap between the state of the art and the current practices in eHealth systems;
- Identification of the actors and requirements for an new identity management model for eHealth;
- Definition of a governance model for an identity management in eHealth, by defining digital mechanisms to secure registration process and user empowerment by allowing the citizen/patient to consent in the disclosure and management of sensitive eHealth attributes.

Furthermore, this research should also be useful to promote fruitful discussions, improve the way applications are currently being developed and provide evidence for the strategic importance that appropriate identity management has for a more secure and reliable eHealth.

1.2 Definitions

To better understand the relevance of identity management for eHealth we must start by discussing concepts such as *privacy*, *security* and *trust* and the place they have in the daily practice of eHealth. Privacy in the context of eHealth is related with the ability of keeping personal information private within the sphere of control of the patient or patient/physician. Identity management plays a key role for privacy protection, because by definition a digital identity in the context of eHealth contains highly critical and valuable personal data.

Digital Identity mechanisms are based on some of the basic fundamental properties of secure systems, namely: (1) message integrity, ensuring that a message or transaction has not been tampered with; (2) non-repudiation, providing evidence for the existence of a message or transaction and ensuring that its contents cannot be disputed once sent, and (3) confidentiality ensuring that only the user or authorized processes can view and use the contents of a message or transaction having access to those contents [5].

For trust there is no real consensus [6]. Trust can be considered as a firm belief in the veracity, good faith, and honesty of another party, with respect to a transaction that involves some risk [5]. Trust is generally linked to a particular set of identity credentials and attributes associated with those credentials. As in the physical world, trust in a digital identity is ultimately based on some set of evidence. The establishment and nurturing of trust is one of the main objectives and tenets of security. Trust cannot be digitally represented or enforced. It can only be nurtured by

giving users confidence on the strength and reliability of the security mechanisms being employed to protect the system integrity and authenticity. Trust can also be granted, adjusted or completely revoked, at any time, leading to some important trust properties [5]:

- Trust is transitive only in very specific circumstances;
- Trust cannot be shared;
- Trust is not symmetric;
- Trustworthiness cannot be self-declared.

Regarding trust, there is a very interesting web-based survey that has been designed to investigate EU citizens' perceptions and attitudes towards the issues involved in eIDs management and interoperability [7]. This survey was translated into 8 European languages and was made available online over a period of one month in June 2006. It got 1,906 valid responses with respondents from 23 out of the 25 EU countries. A limitation of the survey was the number of response rate from some countries was very low and in this respect, the survey was not considered to be fully representative of all European citizens. However, the main results indicated:

- An overall negative perception of the ID authorities by EU citizens;
- The vast majority of the respondents do not trust the relevant institutions; they are seriously critical about the competence of the authorities, and are dubious about their ability to handle personal data with appropriate care.
- Moreover, they are suspicious of the authorities misusing their identity data. These negative attitudes of citizens hold important implications for future attempts at implementing eID cards, as these perceptions may well be translated into subsequent behaviors, namely, resistance to use or, indeed, non-use at all.
- In the countries involved in the survey, the most negative attitudes were found in respondents from the UK and Ireland, and the least negative in Central and Eastern Europe. It was considered in the report, that this may be linked with the particular ID policy and practice mainly, the lack of ID cards in these countries and the high profile public debates that took place in the UK [8-10].

Public trust on a national ID infrastructure is thus dependent on the citizen perception of the competence and care that the legal authorities show on the daily management and handling of personal data.

1.2.1 What is eHealth?

In the nineties eHealth[11] was mainly related with processes involved the transition from paper to electronic based health records. With the implementation of several distributed

environments for eHealth and the increasing need for interoperability between different information systems, eHealth has today a much broader scope. According to G.Eysenbach [12] and also some recent published literature "eHealth is an emerging field in the intersection of medical informatics, public health and business, referring to health services and information delivered or enhanced through the internet and related technologies."

From the point of view of the European Commission, "eHealth covers the interaction between patients and health-service providers, institution-to-institution transmission of data, or peer-to-peer communication between patients and/or healthcare professionals". Health information networks, electronic health records, telemedicine services, wearable and portable systems which communicate, health portals, and many other ICT-based tools assisting disease prevention, diagnosis, treatment, health monitoring and lifestyle management are a few of the examples identified by the European Commission [13].

1.2.2 What is Identity Management?

Identity management (IdM) systems have recently emerged as essential tools directly related with the success of several popular applications; however the concept itself does not seem to have a clearly defined meaning and must therefore be analyzed under different perspectives. Technology-based identity management, in its broadest sense, refers to the administration and design of identity attributes, credentials, and privileges. Together with authentication and authorization models, IdM thus provides a transparent and secure framework for personal attributes interoperability among different applications. Terms and definitions related to identity management can also include beside general terms on identity usage, authentication and authorization concepts, and other identity management terms. For the rest of this document we will employ the concepts and definitions used by the ISO/IEC CD 24760 - Information technology — Security techniques — A framework for identity management [14].

In the digital world an *entity* can for example be a natural person, an organization, or even a software application that requests access to a certain resource. An entity can also have more than one identity. An *identity* is a set of attributes related to an entity. An *identity* is a subset of all possible attributes of the entity. A *resource* can for example be a webpage, data in a database or even an application. To gain access to the resource an entity lays claim to an *identity* [5].

Identities are collections of data about an entity that represent *attributes*, preferences and traits. Attributes are acquired, preferences represent desires and traits are like attributes however they remain unchanged. The term attributes typically means all three unless there is a specific need to distinguish them [5]. *Attribute* is the property or characteristic of an entity that can be used to describe its state, appearance or other qualities.

The use of identity can be for *identification* which is the process to determine if the presented identity information associated with a particular entity is sufficient for the entity to be recognized in a particular domain of applicability. Identification is usually followed by authentication to obtain a specific level of assurance in the result. Other use of identity is *validation* which is the process to determine that the presented identity information associated with a particular entity is applicable for the entity to be recognized in a particular domain of applicability at a certain point in time. Validation usually involves verifying the syntax, and correctness of attribute values, controlling their validity status and matching them with the requirements to recognize an entity. *Domain of applicability* is a point of interaction or set of related points of interaction where an entity can use a set of attributes for identification and other purposes, such as the eHealth context. Identity can also be used as a *profile* which is a kind of identity that contains attributes that are relevant for interacting with one or more distinct domains of applicability. Identity use for authorization is the process by which a temporary set of attributes is added to an identity, thus expressing the granting of a set of privileges to an entity based on policy rules for permitting a certain activity. Authorization often happens in a successful authorization process and the activity permitted after authorization typically involves the access or use of a resource pertaining to the domain of applicability.

The authentication identity can be defined by terms like identity provider, identity authority, credential, authentication, and verifier. *Identity provider* is an entity that makes available identity information. An *identity authority* is an entity related to a particular domain of applicability that can make authoritative assertions on the validity of one or more attribute values in an identity. An identity authority is typically associated with domains of applicability where it can make assertions on attributes that have a particular semantic significance for those particular domains.

Authentication is the formalized process to create a validated identity for a claimant, based on the value of one or more attributes of its identity. *Credential* is an attribute with a value constructed to facilitate validation and to determine the scope of its validity. An authentication identity verifier is an entity that operates the functions necessary to complete authentication. A *verifier* may be the same as or act on behalf of the entity that controls identification of entities for a particular domain of applicability.

Regarding identity management, the terms like: enrolment, identity proofing, identity evidence, identity register, identity registration are important and characterize the management on identity. *Identity management* is defined as a unified set of processes and policies involved in managing the value and life cycle of attributes for the identities of entities known in a particular domain of applicability. These processes and policies in identity management support the functions of an identity authority where applicable, in particular to handle the interaction between an entity for which an identity is treated and the identity authority. The *enrolment* is defined as the process of identity proofing and identity registration that allows an entity to be known within a particular domain of applicability. In general enrolment collates and creates identity information for storage in

an identity register, which is the process of recording an identity in an identity register, to be used in subsequent authentication of the entity in the domain of applicability. Enrolment is therefore the start of the lifecycle of an identity in the domain of applicability for an entity. *Identity proofing* is the initial entity authentication, a particular form of authentication based on identity evidence that is performed as the condition for successful enrolment. *Identity evidence* is the identity information pertaining to an entity required for successful enrolment of the entity.

Identity Management can be classified as: centralized, user-centric or federated.

A centralized IdM treats all identities as known and controlled by one single identity authority. This approach has low complexity but does not give flexibility in accepting entities unless they are first identified under the constraints of the domain of applicability. A centralized identity management may also occur beyond local environments, for instance when governments issue national identity cards for use in multiple scenarios, or in some online single-sign-on schemes.

A user-centric IdM is employed for the optimization of processes for the managing identities in the interest and under control of the end-users. User-centric identity management [14] therefore provides more flexibility by having several identity providers with different identity registries and different identification processes under accredited levels of assurance within a domain of applicability. Each provider acts similarly to the centralized approach but user-centricity provides user rights, not only authority, and mechanisms for exercising control over how some identity attributes are maintained, published and used. For instance, the user's control of attributes may relate to the user's desire for privacy and the validation of user consent. User-centric identity management seeks to place administration and control of identity information directly into the hand of users. Examples include network "*anonymization*" and/or "*pseudonymisation*" tools, and requirements that minimize the disclosure of personal information, or password managers that securely keep track of different credentials. For example, in the real world, a wallet full of different identity cards can be seen as a user-centric form of identity management that allows individuals to choose the appropriate identity credential for the right purposes, such as a patient identification number or professional card. This way, users can exercise direct control over how personal information is disclosed to and used by information systems.

The federated type [14] of IdM is used in situations where entities need to act outside of their original contexts in a third party domain where their identity cannot be directly validated. Within an identity federation, entities can act under these conditions without the need for a new identity and identification for the third party domain of applicability.

All three types of identity management systems are usual necessary, depending on the context and requirements of the application, and they can also complement each other. Usually identity is considered to be highly contextual and people use their different forms of identification for different contexts where they can be appropriately accepted and validated.

The *identity life cycle* provides an overview of the different states an identity may be during its existence, and the possible transitions between these states. An identity lifecycle is the combination of these states along with the associated transitions.

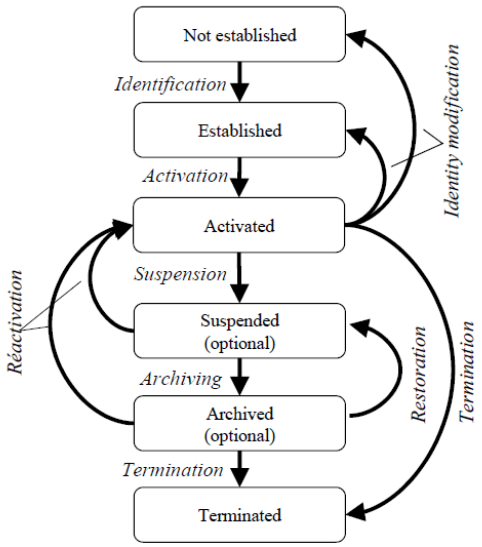

Figure 1. Identity lifecycle - ISO/IEC CD 24760

The different states typically recognize an identity as:

- **'Not Established'**: an entity is not recognized in a domain of applicability. In some cases the entity exists, and in others the entity does not exist. For example in the eHealth domain, the user might not be recognized even if the user has a social security number assigned.
- **'Established'**: the identity of an entity is recognized in the domain of applicability but the entity is not yet able to interact with other entities in the domain of applicability.
- **'Activated'**: the identity of an entity is recognized in the domain of applicability and the entity is able to interact with other entities in the domain of applicability according to the purposes of the domain of applicability.
- **'Suspended':** this is an optional state, as the identity of an entity is recognized in the domain of applicability. However, the entity is no longer able to interact with other entities in the domain of applicability.
- **'Archived' (optional)**: an entity is no longer recognized in a domain of applicability but records may need to remain available to determine whether or not an entity has in the past been recognized in a domain of applicability with a particular identity.
- **'Terminated':** the identity of an entity is no longer recognized (or necessary) in a domain of applicability.

In the case of hospitals, identity management is usually carried out in accordance with the central model, where system administration assigns "log on" credentials to its users to facilitate and control access to local sensitive resources. However when one of the users leaves the hospital, his "log on" credentials and associated privileges (identity) should be revoked by system administration. This is often called provisioning and deprovisioning. Figure 2 represents the main processes that are associated with identity management in IT systems.

Provisioning in eHealth is the process of preparing an IT system to provide service to a health care professional, patient, or other authorized users. From the perspective of digital identity, provisioning is the creation of the identity record and its population with the correct and appropriate attributes. These attributes might be standard items, such as name, location, email, and phone, as well as items more specific to the system like patient ID number, etc.

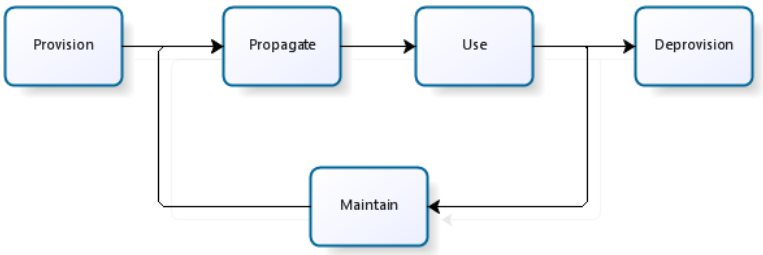

Figure 2. IT system identity management lifecycle

Provisioning can be done through a system administrator or by the user using self-service. Self-service mechanisms are automated process for user auto-enrolment.

Self-service provisioning started to be used on internet services, and it a nice and perfect solution for huge amount of users for services delivered over the network. Self-service or auto-enrolment provisioning is considered to work well where there is little need to verify credentials other than perhaps a credit card [5]. Then depending on the IT Systems, identity propagation to other systems is part of its lifecycle. For simple systems, the propagation is as simple as writing the identity information directly in a local file or storing it in a local database. More complex systems may provide some sort of shared identity directory where the identity created in one place can subsequently be used in multiple systems [5].

After the provision and propagation phase, the identity can then used by various systems and agents. This might be as simple as consulting the identity to authenticate and authorize user actions when access is requested to resources. In the "maintain" phase, and regarding the nature of the identity, attributes will change from time to time, either because the base attributes of the entity change, because roles and assignments may change or new attributes are needed for new or updated

applications. It is therefore normal that according to business opportunities or other circumstances, the schema of the identity record may need to be changed to contain new fields to or include entirely new systems.

The deprovisioning process is responsible for removing users from the system leave the organization finishing their identity lifecycle. It is considered that deprovisioning is as important as provisioning, because active users left in the system that have no longer authorization to access the system can be potentially danger. Usually failures in user deprovision can lead to serious impact even to fraud or theft. Failures in deprovision is one of the common breaches faced by many organizations [5].

1.3 Assumptions and scope

The scope of the thesis is to define and propose an identity management model for eHealth. Its application in other domains is not considered nor discussed.

It is assumed that all citizens have an eID card. In Portugal, the eID will become mandatory in 2014, until then the use of other identification cards such as "*Bilhete de Identidade"* and "*Cartão de Utente"* are legal. For the electronic identification it is required and assumed the existence of an eID. In the present model it is also assumed that all eID cards also have included the patient ID number. However it is known that for Portuguese that live abroad, the local Portuguese Consulate registers and issues eID cards without a patient ID number. The use of these eID cards are considered out scope for this work.

The definition of the patient registration in the national health system is not included in this work. We assume and base our work on the existence of a reliable registration of patients, responsible to assure the existence of strictly non-duplicated patient ID numbers that can act as a reliable source of truth.

In our proposed model the definition of full set of identity attributes for eHealth is out of scope and is the subject of future work. This decision was taken because the collection of a more complete set of useful identification attributes for eHealth would necessarily imply a huge effort on our part and some time to mature, which is clearly incompatible with the restrictions of time we had available to terminate this work. It would also require the involvement of several experts in several different domains.

The secure privacy oriented identity infrastructure we propose fits well within the highly demanding and specific needs of a heterogeneous and integrated modern identity infrastructure for eHealth applications, precisely because it provides strong foundations, upon which more reliable, secure, trustworthy and interoperable eHealth applications can be built.

2 IdM IN HEALTH CARE

This chapter describes the evolution of identity management in eHealth by taking into account: (i) An historical perspective of Identity in eHealth information systems from its beginnings in Portugal, (ii) A literature review: Issues and future perspectives on Identity Management in eHealth.

The beginning of the patient identity in health care is framed with a brief background history of the early health information systems in Portugal, identifying and describing the most important and structural health information systems that provided support and lead to the establishment of the National Patient Identifier.

2.1 Historical perspective on patient ID in eHealth

Patient identification in the Portuguese NHS was initially made via the patient ID Card. This patient ID card was launched in 1995 [15]. In 1995, the existences of different methods to register patient's identification, and sometimes these could lead to a bad identification and not correspond to the right person. Beside patient safety this misuse identification, this could also lead to bad identification in patient benefits in NHS. These problems constitute a strong evidence for the need to create a better identification in NHS by promoting the patient health card called "*Cartão de Utente"*. With the evocation of universality and equity to health care, came the creation and free issuance of the patient identification card of the National Health Service, with an opt-in policy.

The method for obtaining the patient identification card was by registration in primary health care. The enrolment process allowed that the registration process could be made by the patient itself or by a family related individual. The patient card issuance was not immediate, it was done by "*Imprensa Nacional Casa da Moeda"* [16] and it could take months to deliver the patient card to patients. Meanwhile patients could identify themselves with the provisory registration paper with no additional security measures applied while waiting for the card to arrive.

The process of issuing a duplicate card was provided in case of loss, destruction or theft, however its revocation has never implemented. Since the patient card did not have visual identification characteristics and by law no other documentation was required to identify a patient in health service, patient ID theft and fraud could easily occur.

More recently the patient ID card has been replaced by the Citizen ID Card called "*Cartão de Cidadão"* (CC) in 2006/7. The citizen ID card is an easy to use electronic and physical document, allowing for the identification of citizens through various channels of communication, face-to-face or remotely based and for Public Administration and private entities services [17]. It replaces

several other ID cards, such as the identity card ("Bilhete de Identidade"), Fiscal card, social security number and patient ID card.

Technologically, the Citizen Card is compliant with the more relevant international standards, particularly at European level. It takes the form of a smartcard card with a tamper proof microchip embedded with storage capacities and capable of information and cryptographic processing, which ensures the highest safety standards in protecting the confidentiality and integrity of personal information of citizens, respect for national laws and corresponding European standards.

For national citizens, resident in Portugal or abroad, the Citizen Card is mandatory. The citizen card is also mandatory for children from six years of age or younger, if the card presentation is requested by any public service.

Requirements for the registration process of the CC depends on several situations, e.g. age, if the enrollee is a foreign resident or a national citizen, but for all cases the registration process requires the citizen physical presence both during initial registration and for the final delivery of the card.

2.2 Literature review: main issues and future perspectives on Identity Management in eHealth

In this section, we present the literature review search strategy, query definition, study selection criteria and study characteristics defined.

2.2.1 Literature review search strategy

A comprehensive literature search was conducted on PubMed and IEEE Xplorer to identify relevant published articles. The keywords that were used include identity, identity management, identity-management and identification, authentication and authorization. These terms were used in combination with eHealth, e-Health or electronic health.

We have used the following search query:

("identity"[All fields] OR "identity management"[All fields] OR identity-management[All fields] OR ("identification"[All fields] AND authentication[All fields] AND authorization[All fields])) AND (eHealth[All fields] OR e-health[All fields] OR "electronic health"[All fields])

For the search query results, the criteria required for relevance and inclusion in our literature review were: (1) be published in the English language, (2) approach or somehow cover identity in eHealth, (3) articles available in full text.

2.2.2 Study selection

The titles and abstracts of the identified relevant papers have been carefully analyzed. Studies that cover identity, but with general reviews and not focused on identity management in the context of eHealth were excluded. This exclusion criterion was used because the primary aim of the review was to provide an identification of the main findings, issues and future perspectives on identity management in the eHealth context and articles targeting other application areas other than eHealth (e.g., information society) were beyond the scope of this review.

We have also manually examined the references cited by relevant selected papers to identify additional articles for our literary review.

2.2.3 Study characteristics

The selected studies focus different populations and different contexts, from local to national. Since identity management covers several different areas of knowledge and different perspectives, selected studies were grouped into themes, based on the main area of each study and its main findings.

2.2.4 Results

We start by giving a general overview and a thematic analysis covering these differences followed by the main issues and future perspectives that have been identified in the literature. We end by describing the main research programs and working groups cited in selected studies identified in the literary review.

Our search criterions identified 17 articles in Pubmed and 14 articles in Xplorer database. Figure 1 represents the results obtain following the methodology described.

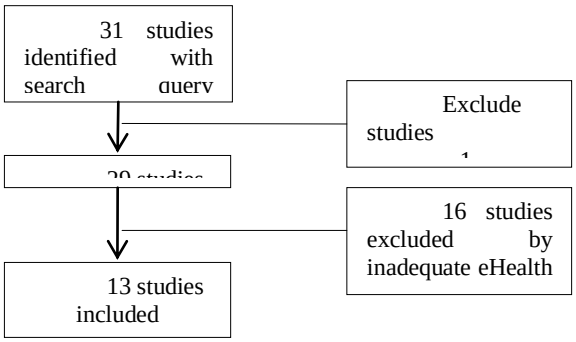

Figure 3 Results with search methodology

Table 1 shows the total of 13 studies included in this review. Most of the work described has been conducted in Europe (69%) and Australia (15%), and the majority has been conducted in the past three years (85%). We have not been able to find any relevant work conducted in the United States related with identity management for eHealth.

These studies approach identity management from different perspectives and enabled us to identify key themes, based on our main study subject. The research themes thus identified were: identification, authentication and authorization identity in eHealth (three studies); identity pseudonymisation and anonymization for secondary use electronic health records and personal medical records (two studies), privacy preserving identity (four studies) and identity and standardization (four studies). References and citation from other included studies can be included in thematic analysis.

Overall, the main population focuses on Identity management are patients and healthcare professionals. Only one study [18] is focused on healthcare professionals, in a strictly local context for the purpose of identification, authentication and authorization. All the other studies where cross context, from local to national environments, and from private networks to public networks such as the Internet.

Table 1 Profile Identity Management in eHealth Studies.

	IPASU	PPI	IAA	IS	Total
How many?	2	4	3	4	13(100%)
Where?					
Europe	2	2	1	4	9 (69%)
Australia		1	1		2 (15%)
Canada		1			1 (8%)
India			1		1 (8%)
When?					
2009			1		1 (8%)
2008		3		3	6 (46%)
2007	1	1	2		4 (31%)
2006				1	1 (8%)
2004	1				1 (8%)
With whom?					
Patients	2				2 (15%)
Professionals			1		1 (8%)
All		4	2	4	10 (77%)
Context?					
Local	2			1	3 (23%)
Cross Context		4	3	3	10 (77%)

IPASU - Identity Pseudonymisation and Anonymization Secondary Use

PPI - Privacy Preserving Identity

IAA - Identity, Authentication and Authorization

IS - Identity and Standardization

In general the identified studies describe prototypes and models with only one study presenting the experience of a real deployed implementation[19]. Some studies are also based on the results obtained by research projects funded by European Commission [20].

2.2.4.1 Thematic analysis

In this section, some thematic analyses from the results of the review are presented, grouped by the themes previously identified.

2.2.4.1.1 Pseudonymisation and anonymisation identity for secondary use

Pseudonymisation is a procedure by which the attributes that can identity a person identity are replaced by one or more artificial identifier's [21]. There can be a single pseudonym used of multiple pseudonyms. Pseudonymisation is used to protect patient privacy data. Data in this form is suitable for extensive analytics and processing for secondary use such as epidemiological research,

finance and others. Anonymisation [22] is a result of not having identifying characteristics disclosed and is very different from pseudonymisation, because pseudonymisation allows tracking back of data to its origins, where in anonymisation all person-related data that could allow backtracking has been purged and cannot be reconstructed from the available data.

This section presents the results of a literature review, and also information on the latest work that is being done in this area.

2.2.4.1.2 Literature review

The pseudonymisation and/or anonymisation of electronic health records for other usage of personal medical records, is essential to ensure the protection of private and personal data. Especially when it leaves the control and the protection sphere of the health care services, for other secondary uses such as clinical or epidemiological and health care research projects, assessment of treatment quality or economic assessments [23]. For these uses, in general the patient identity is not needed, and therefore the data must be anonymised or pseudonymised. In what follows we present relevant technical approaches for pseudonymisation and anonymization for preserving patient identity privacy. Whereas for the one-time use of the data the procedure for anonymisation is straightforward, long term data accumulation or the need for a re-identification process requires a more sophisticated approach[24].

2.2.4.1.3 Recent work in pseudonymisation

In 2008, the ISO/TS 25237:2008 [25] was released and it contains principles and requirements for privacy protection using pseudonymisation services for the protection of personal health information. ISO/TS 25237:2008 is issued as technical specification and not as a standard that should be used by organizations who make a claim of trustworthiness for operations engaged in pseudonymisation services in eHealth. Technical specification must be reviewed at least every three years to decide whether to confirm the technical specification for more three years or to revise its status to became an international standard or simply withdraw it. After six years, a technical specification should be converted into an international standard or withdrawn.

This technical specification defines one basic concept for pseudonymisation and gives an overview of different use cases for pseudonymisation that can be both reversible and irreversible. The document also specifies a base policy framework and the minimal requirements for trustworthy practices for the operations of a pseudonymisation service, a policy framework and minimal requirements for controlled re-identification and also specifies interfaces for the interoperability of the associated services interfaces.

Following the article 29 of the Data Protection working party[26], pseudonymisation and other de-identification practices are recommended. This technical specification is considered to be the first of its kind, and it constitutes a solid foundation for potential and future related standards[27].

2.2.4.2 Privacy preserving identity

When considering access to eHealth systems and the sharing of personal health information in distributed systems within different organizations, security and privacy must be addressed, in particular, compliance with the relevant privacy legislation must be guaranteed. Some solutions are pointed out, such as federated identity management, that can enable users and service providers to securely and systematically manage identities and user profiles in a single sign on framework that controls access to personal information [28]. However, federated identity management presents a specific privacy threat because it makes intensive use of identity information [29] flowing between different administration domains. Information is exchanged cross-context, and for identity protection, identifiers mappings and conversions are required.

Several studies point out that the mapping translation should be performed by a trusted third party and it should be available for all the communicating contexts [29]. This trusted third party should be a legal organization responsible for the approval of reversible identity, aiming to protect the privacy and security of identity.

A key component for user privacy is preserving the user's ability to remain anonymous [30]. Anonymisation can represent a threat because accountability is important in data security management and if the user is anonymised it is difficult to assure security and privacy while allowing health record data to be accessible by authorized people [30].

Some architectures for the preservation of privacy in eHealth allow different uses of identifiers called pseudonyms in different medical contexts to preserve the users privacy. Sensitive medical information can be collected from distributed health record databases in different health organizations and linked together dynamically without revealing the consumer's real identity using concepts like identity management. This architectural design also allows the revocation of anonymity under well-defined policies with legal-compliance [30] and prevents disclosure attacks and statistical analysis [31]. Sharing medical data on large scale can also expose patient privacy-related threats, such as massive data aggregation or profiling [29].

Also, a user centric identity management and a technique called obfuscation can be used to prevent identity disclosure attacks and statistical analysis. This improves the privacy of patients enormously by applying additional methods of anonymous authentication and privacy. These issues are referred especially on eHealth portals and as a countermeasure it is proposed the use of identity management. In this context identity management can be described by means of dividing the identity of a person into several sub-identities to pseudonymised, obfuscation and anonymous authentication [30].

Other studies observed that role based access control for granting access to medical information is less central than expected in deciding whether an access request to medical information should be granted or not. Because relationships between patients and health care

professionals exist, other context-dependent parameters, such as time and location, should be considered and evaluated for the authorization process. In all these cases the establishment of identity of the involved parties is often a primary pre-requisite for authorization to be granted [29]. An interesting result of this study [29] is that role-based access control is not enough in the federated eHealth scenario. There are several cases where verifying identity, rather than role-related credentials, is a pre-requisite to the enforcement of cross-context eHealth authorization rules.

Some of the issues related with privacy preserving identity are related with (1) leveraging Internet technology to provide health workers access to electronic health records requires security and privacy to be addressed, in particular, compliance with the relevant privacy legislation [28], (2) concerns about the right of healthcare consumers to protect their privacy in the e-Health system [30], (3) a key component of user privacy is preserving the consumers right and ability to remain anonymous, However, anonymity affects many security requirements, such as accountability, authenticity and non-repudiation[30], (4) since eHealth portals can be accessed via the Internet, security and privacy issues arise and have to be considered carefully, threats such as the trivial disclosure attack and the statistical analysis of metadata [30] can be done, (5) sharing of medical data on a large scale exposes the patient to several privacy-related threats, such as massive data aggregation or profiling [29], (6) state-of-the-art solutions provide inter-operability by means of a mediator component that maintains a look-up table storing all local identifiers across contexts - this may lead to potential privacy threats and data aggregation. An attacker can obtain (illegitimately) the information that is used by the mediator in order to map references across contexts. In this circumstance, the attacker is in a privileged position to correlate patient's information on a large scale [29].

2.2.4.3 Identity, authentication and authorization

Identity, authentication and the authorization level depends on who is getting the access, and different levels are defined for different resources. Attribute certificates, identity certificates, patient consent are important mechanisms to define more fine grained rules for the granting of access.

Medical data security is an important issue that poses technical, organizational and ethical challenges [32]. The access control policies and mechanisms required to access medical data must not only ensure that sensitive patient data is accessible to the authorized personal only, but also assure that it is immediately available when it is needed in life critical situations.

Some of the studies [33, 34] propose systems that are able to define access control rules using a combination of standard, identity and authorization credentials, thus simplifying the specification of appropriate access control policies. Standard credentials are quite versatile and a single credential can grant access to a variety of data sources to the user. Using standard credentials provides access to a large number of users possessing the same type of standard credential. However, the use of associated attributes with the standard credentials considerably helps in

achieving the required fine grained access control. The user based accesses in an administrative domain can be easily handled using identity credentials. Authorization credentials are usually useful in providing situation based one-time access to specific items.

Another important issue that is addressed [35] is when eHealth systems can be used anywhere, through Internet access. In order to know that the right person is getting access to the right record anywhere, a strict identity check is needed and cryptographic techniques, such as those of public key cryptography and associated keys infrastructure should be use. This will not only help to ensure the authentication of the requests sender and the integrity of the data but also the protection and confidentiality of the access.

The main findings, issues and future perspective, related with identity management in the eHealth context with identity, authentication and authorization are: (i) Most of the existing access control approaches make use of either identity credentials, attribute credentials or authorization credentials. In an Identity based access control system, a doctor can access the details of his own patients by submitting the appropriate Identity Credential, but an unknown doctor will fail to access the patient's critical data when needed. [33]; (ii) Future work also incorporates design of appropriate infrastructure for issue and management of various credentials [33].

2.2.4.4 Identity management and standardization

Considering the threats related to security and data protection in eHealth, the following areas should be considered [34]: (1) the access to the information, (2) its transfer considering communication infrastructures and (3) the recording and archiving of sensitive information. Since each country has its own national standards, these need to be harmonized at the European and international levels.

EHealth and identity represents much more than just a simple change from paper based records to electronic records. As identified previously in several studies, interoperability becomes a critical issue and data security and confidentiality are vital for acceptance of new approaches and to support eHealth [34] in a secure way.

Several standards are under development for Health Informatics and associated security domains, such as ISO/TC215, with the scope defined for standardization in the field of information for health, and health information and communications technology (ICT) to achieve compatibility and interoperability between independent systems. Also, to ensure compatibility of data for comparative statistical purposes (e.g. classifications), and to reduce duplication of effort and redundancies[36].

CEN/ISSS promoted a work group, with focus on eHealth standardization, to investigate standards requirements in the area of eHealth with connection with eEurope2005 Action Line. The final report "Current and Future Standardization issues in the eHealth domain: Achieving

Interoperability" [37] contain some recommendation for future priorities for eHealth standardization activities.

A new framework defining identity management is under development by the International Organization for Standardization, ISO/IEC CD 24760 - Information Technology, Security Techniques, A framework for identity management[14]. This standard aims to provide a framework for the definition of identity and secure, reliable and private management of identity information. Other relevant ISO committees activities under the group of security techniques[34] are: TC46/SC11, TC68/SC2, TC68/SC 7, TC204, TC 215, TC223, TC246, TC247.

Standardization is needed to provide interoperability between different eHealth systems, providing privacy and security to identity exchange information and better controlling the processes of observability, linkability, data aggregation and profiling [34].

Significant work has been done on standardization, but many of the results are not known to the user nor has their usability been fully evaluated. Standardization bodies are urging input from users [34]. Identity management and new technologies like biometric sensors, RFID or NFC for tracking are on the verge of being introduced [34] and their real impact on identity and the privacy of the user needs to be better evaluated on real case scenarios.

2.2.5 Research programs and working groups identified in literature review

BioHealth and the Liberty Alliance are research programs, focused on identity. Some of their main results and future perspectives are presented in several articles [28, 34].

The BioHealth [36] project was funded by the European commission to address security and identity management standards in eHealth, promoting awareness, knowledge and understanding of privacy issues and existing and emerging security standards in the area of eHealth.

Some of the issues, findings and results [34], by the BioHealth project are: (1) the citizen has to take more responsibility, (2) new technologies and its impact have to be evaluated, (3) the quality of communication and data access needs to be assured, therefore, systems have to be both secure and reliable at all levels, (4) systems have to be interoperable and this requires the use of standards, (5) strong Identification methods, have to ensure that the information can only be accessed by the entitled person, (6) patient free mobility is strictly correlated to the access and retrieval of medical data and this is one of the more delicate issues in terms of data protection.

The Liberty Alliance [38] project was established in 2001 as a consortium of technology vendors. The project vision is "Liberty Alliance is to enable a networked world based on open standards where consumers, citizens, businesses and governments can more easily conduct online transactions while protecting the privacy and security of identity information" [38]. A key concept in the Liberty Alliance project is a "Circle of Trust", in which federated identity management is used

to create a business to business network (B2B) of cooperating enterprises that provides integrated services to users[28].

In Australia, electronic health implementation [30] was promoted, through the HealthConnect scheme and more recently through the Australian National e-Health Transition Authority [39]. NEHTA's work was focused on a shared electronic health record and national solutions. To address this, the project employed unique identifiers for patients and clinicians and agreed upon a standardization on terminology, e.g. SNOMED. NETHA's expectation is that through such initiatives this research on consumer-centric identity management will be able to gain acceptance [30].

The EHIP [29] research project developed a security architecture based on a multi-party shared platform. The platform is a communication infrastructure that allows many healthcare providers to collaborate by sharing the medical information they produce.

2.2.6 Discussion

The aim of this review was to identify key issues and future perspectives by evaluating the literature on identity management in the context of eHealth and by gathering and synthesizing information from primary studies.

Considerable research has been made in the last three years (11 studies). Based on the literature, the identified research was essentially made in Europe and the main interest was in exploring different architectures and models that can be implemented in the future with identity management in eHealth, based on a patient's centric approach.

Significant evidence has been found highlighting major issues in dealing with identity, especially in the context of eHealth, because of the sensible information, data security and associated privacy. On the other hand, legal barriers on the exchange of identities information show the need to research new compliance architectural and models. In general, very few studies have been really implemented. This is an indicator that identity management in eHealth is much more complex than it seems and that, reliable and trustable, data security and privacy are very difficult to achieve in the real world.

Several research projects are currently being developed within the context of eHealth, to be able to define standards for identification process using ICT technology. A Trustable identification process is needed and standardization needs to be further developed.

Considering the patients and healthcare professionals mobility and that the access should be granted anywhere, several research groups are defining standards to provide interoperability between different eHealth systems. The standards should provide privacy and security related with

identity exchange information and the control of key issues such as observability, linkability, data aggregation and profiling.

Another aspect related to identity and standards is gathering medical data for secondary use on medical and epidemiological research. Methods for anonymization patient identification and reversible identification are needed. Linkability is also needed to provide more research information. Different methods and architectures were proposed, and all were concerned with assuring a trustable and independent entity. This entity should map the identities and anonymise identity information.

There is no consensus and no standardization methods for the anonymisation of identification for research purposes. Requirements for protecting identity and related attributes should always be defined in architectures and models proposed in and eHealth context.

Furthermore, the studies examined in this review presented consistent findings related to the architectural model focus on patient centric and on federated modes for identity management.

EHealth allows patients to actively participate in the process of health care, improves their awareness and feeling of security, and ultimately leads to their empowerment. Nevertheless, there is no evidence found on the acceptance of patients and health care providers on the use of trustable mechanisms and models on identity management to provide enhanced security and privacy. Attitude and behavior for patient and health care providers related with identity management in eHealth should be considered for further research.

2.2.7 Conclusion on the literature review

Identity management is a key component for eHealth. The need for a standard methodology for identity and authentication interoperability between the different stakeholders in eHealth has been identified. Although several research efforts have been found in the context of identity management for the information society, very few studies and experiences were found for a strict eHealth context. Since eHealth deals with very sensible information there is a real need for further research work showing evidence that privacy and security can be really achieved for interoperable eHealth systems. Very few implementations could be found in the literature, showing that this problem is even more complex than it seems and future adoption requires further research on new models and architectures assuring the eHealth stakeholder's acceptance.

Legal and security issues associated with availability, integrity and confidentiality, related with identity in eHealth, were expected to be found in the literature. However no such themes were found. These are important themes that should be further discussed because they are the main barriers for the implementation of identity management in the context of eHealth. Consensus and acceptance between all stakeholders on policies, processes, and technologies should be promoted, allowing for the building of a circle of trust to allow users access to eHealth applications and

associated information resources, that assure the protection of confidential and personal information from unauthorized access within different authentication contexts.

3 STATE OF THE ART ON IdM

Healthcare professionals and patients need a secure, convenient and effective way of identifying themselves, replacing signatures and stamps used on paper [40]. There is a strong commitment and investment in European Union to make this a reality in the information society, and it is being spent about tens of billions of Euros in interoperable electronic Identity Management (eIDM) [40].

To characterize the state of the art, we analyze several projects funded by the European Commission clearly stating the best of knowledge on Identity Management in information society, some of them establish scenarios in eHealth domain. The models introduced by these projects are being implemented in real world scenarios on the information society context. Since there are so few studies in the eHealth context regarding eIDM, eHealth will arrive later to the problem, facing directives and laws that are already published without criticism and discussion promoted from the health context. This chapter presents some of the findings of these projects that can reflect the state of the art outside the eHealth domain. This will give some intuition to understand how this subject is being treated and the needs that should be considered in the eHealth context, identifying the gap between the needs in information society and health domain.

At the end of this chapter, a review over the open standards available are described and a briefly comparison is made.

3.1 The law and regulation

In this section the most relevant regulation and laws are identified, and the proposed model must be compliant with the national and European legislation.

3.1.1 National law

In Portugal, data protection is assured by national legislation that address personal and Health data service provision and is conducted by national authority called 'Comissão Nacional de Protecção de Dados' (CNPD). This commission produced some legislation on personal data protection [41] and Personal genetic information and health information [42]. However there is no legal framework specific for eHealth or for telemedicine practice, although these have to comply with the general personal data protection law.

On the other hand, clinician practice is regulated and managed by "Ordem dos Medicos" [43]. In order to guarantee the basic right to patient's life privacy and especially to health data

confidentiality, all healthcare professionals are under the duty of confidentiality, for instance nurses' deontological code [44] and physicians' deontological code [45].

Clearly, physicians and nurses represent a very significative and important part of healthcare professionals, however there are many other professionals that interact with patients that don't have their own deontological code defined.

Article 35º of Portuguese Republic Constitution [46] defines that patients in Portugal have the right to be treated with privacy. Also the National basic law for health care assures the citizen/patient right to be treated with privacy while respecting personal data confidentiality [47]. Health services are available to everyone and can be delivery by public or private entities, and are regulated by the health public sector.

On the penal perspective, the articles 192º and 193º of Penal Code define the responsibilities for crimes against life privacy or its attempts [48].

Law n.º 247/2000 from the 8th of May [49] regulates Hospitals' archive norms, however don't considers digital data archives.

3.1.2 European directives

The European Parliament and the Council of 24 October 1995, established the data protection directive 95/46/EC "on the protection of individuals with regard to the processing of personal data and on the free movement of such data" [50]. This directive was transposed into the Portuguese legal system with the implemented law 67/98 of 26 of October "Law on personnel data protection, relating to treatment and circulation of personal data about individuals".

Several recommendations/directives have been defined, for data protection, privacy and confidentiality with special emphasis to the following:

- Recommendation R (97) 5 of the Committee of Ministers to Member States on the Protection of Medical Data and Explanatory Memorandum to Recommendation No. R(97) 5;
- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a "Community framework for electronic signatures";
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 "concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communication)";

- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000, ”on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("e-commerce Directive")”;
- Directive 1999/93/EC - Decree-Law no. 290-D/99, of 2 of August. Legal rules governing electronic documents and signatures, modified by Decree-Law no. 62/2003 of 3 of April and Decree-Law no. 165/2004 of 6 of July;
- Directive 2002/58/EC - Law no. 41/2004, of 18 of August. Legal provisions transposing to the national legal order Directive 2002/58/EC, of the European Parliament and of the Council, of 12 July, concerning the processing of personal data and the protection of privacy in the electronic communications sector;
- Directive 2000/31/EC - Decree-Law no. 7/2004, of 7 January - Transposing into the Portuguese legal system Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market;
- Recommendation No. R (97) 5 – included in the Law no.12/2005, of 26 of January, which envisaged also to comprise the recommendation' guidelines about protection of medical data envisaged also to comprise the recommendation' guidelines about protection of medical data;

The European Union also issued directives such as 36/2005 on professionals regulation and their recognition [51] and guidelines for patient data protection [52]. Directive 36/2005 [51] determines that the free movement and mutual recognition of qualifications of doctors, nurses responsible for general care, dental practitioners, midwives, pharmacists should be based on the principle of automatic recognition of qualifications, based on the coordination of minimum training conditions.

3.2 Laws of identity

Law of identity [53] were developed through an open consensus process among experts and stakeholders, reflecting a remarkable convergence of interests, and are non-proprietary in nature. As a result, they have been endorsed and adopted by a long and growing list of industry organizations, associations, and technology developers.

The driving force for Laws of identity was the well accepted knowledge that “The Internet was built without a way to know who and what you are connecting to” [53]. Laws of Identity is project to develop a formal understanding of the dynamics causing digital identity systems to succeed or fail in various contexts expressed as the Laws of Identity. Considering all together, these

laws define a unifying identity metasystem that can offer the Internet the identity layer, and establish the fundamental rules that the identity systems implementation should obey.

Laws of identity defined 7 fundamental rules that any identity system should obey, namely : (1) user control and consent, (2) minimal disclosure for a constrained use, (3) justifiable parties, (4) directed identity, (5) pluralism of operators and technologies, (6) human integration, and (7) consistent experience across contexts.

Although, the laws of identity were establish for the Internet context, they can be applied to more demanding contexts, such as eHealth with more issues and needs. We now establish the relation between the contexts and the fundamental rules on the Laws of Identity:

1. **User control and consent**: "*Technical identity systems must only reveal information identifying a user with the user's consent*". By legal right, established by law 67/98, 3rd article: h) "Consent of data subject means any manifestation of will, freely given specific and informed, pursuant to which the owner agrees that their personal data being processed" [41].These law were transposed to national law by the European directive 95/46/EC [52]. The consent is also regulated by law over the personal genetic information and health information law establish by law 12/2005, "Access to health information by its holder, or others with his consent, is made by a doctor, cleared itself, chosen by the owner of the information." [42]. This leads to the opportunity for patient empowerment allowing the patient to know who is accessing his information, what eHealth services are being delivered, and manage the consent when attributes are disclosure between different parties, deciding and controlling to supply identity information, and have no doubt that it goes to the right place. With the identity system provider patient's trust and so empowerment will raise. To remember user decisions, the metasystem should have mechanisms that store information and users may opt to have them applied automatically on subsequent occasions. This gives the opportunity to have user profiling information threading his privacy.
2. **Minimal disclosure for a constrained use**: "The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution." The approach is to acquire information only on a "need to know" basis, mitigation the risk of possible damage when unauthorized information is disclosure. Having only the necessary information, the minimalist principle of information, is therefore a less attractive target for identity theft, profiling and should reduce the risk even further.
3. **Justifiable parties**: "Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship." – Only those parties authorized to access the data, because

they are justifiably required to do so, are granted access. This is in sequence of minimal disclosure and the "need to know".

4. **Directed Identity**: "A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles."
5. **Pluralism of operators and technologies**: "A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers."
6. **Human integration**: "The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks."
7. **Consistent experience across contexts**: It is expected that consistent experience exist even if different contexts are applied. For the user, this should be transparent operational and technological functions that are required even though consensus have to be accepted between different parties.

3.3 STORK Project

The aim of the STORK [54] project is to establish a European eID Interoperability Platform that will allow citizens to establish new e-relations across borders, just by presenting their national eID. The STORK project vision is in the future, European citizen should be able use national eID to access services online, and the platform should be able to obtain the required guarantee authentication from governments [54].

The role of the STORK platform is to identify a user who is in a session with a service provider, and need to send his data to this service, this data might represent some personal attribute data, and whilst the service provider may request various data items, the user always controls the data to be sent. This brings the concept of explicit consent of the owner of the data, which is the user, and it is always required before his data can be sent to the service provider.

The state of the art on identity management brings the concept of user-centric approach. This approach is the most important condition for privacy assurance [55] since the user have to explicitly give consent to exchange personal data to the service provider and the platform does not store any personal data, so no data can be lost or profiled. So, the user centric approach is in line with the legal requirements, to protect personal data, establishing concrete measures to be taken to guarantee that a citizen's fundamental rights, such as his privacy, are respected [55].

3.4 Prime – Privacy and Identity Management for Europe

With the shift from a paper-based to an electronic-based services, it became common to profile individuals in order to present more personalized information [56]. It can be considered that while such profiles can be helpful, improve efficiency and empower patient with the personal data information, they can also govern or potential govern opaque decisions about an individual's access to services, in many cases, profiling the patient information need, and so disclosure personal data is done without the consent of the target patient.

Enhanced-privacy is proposed in PRIME [57]- Privacy and Identity Management for Europe, prototype. The project aimed to develop a working prototype of a privacy-enhancing Identity Management System.

European Union has promoted a directive that have been implemented by European member states to provide a legal framework guidance [52] on processing of personal data, this directive was transpose to national law on personal data protection [41] with the specific aim to empower the citizens control over their data. PRIME project, complement the legal framework into a technical framework [57].

The PRIME vision, shares some of the defined concepts of Laws of Identity[53]. Regarding accountability the PRIME vision establishes the following goals: (1) user informed consent and control, (2) privacy negotiation and dispute handling, (3) data minimization and identity management, (4) spectrum of anonymity and pseudonymity on explicitly agreed term between all the parties.

3.5 PrimeLife

Primelife is a research project funded by the European Comission's 7th Framework Programme with main goal to bring sustainable privacy and identity management to future networks and services. Primelife consider that "*individuals in the Information Society want to protect their autonomy and retain control over personal information, irrespective of their activities. Information technologies hardly consider those requirements, thereby putting the privacy of the citizen at risk. Today, the increasingly collaborative character of the Internet enables anyone to compose service and contribute and distribute information. Individuals will contribute throughout their life leaving a life long trail of personal data"* [58].

These are substantial new privacy challenges and Primelife technical challenge is how to protect privacy in emerging Internet applications such as collaborative scenarios and virtual communities, and second challenge is how to maintain life-long privacy.

The project expects working in substantial progress in many underlying technologies. and will substantially advance the state of the art in the areas of human computer interfaces, configurable policy languages, web service federations, infrastructures and privacy-enhancing cryptography.

PrimeLife produced a wide variety of results and the main results are grouped by the different PrimeLife activities [59]:

- Privacy for Life – New Concepts for Privacy
- Privacy-Enhancing Mechanisms
- Policy Languages, Authorization and Access Control
- Human Computer Interactions
- Infrastructures and Privacy
- Standardization, Education, and Open-Source

3.6 FIDIS - Future of Identity in the Information Society

FIDIS [60] is a research project funding by the EU's 6th Framework Programme in European Information Society (EIS) which address trust, security and preserving the privacy of individuals.

The project vision was that Europe should develop a deeper understanding of how appropriate identities and identity management could point the way to a fair(er) European information society.

FIDIS main objectives are shaping the requirements for the future management of identity in the European Information Society (EIS) and contributing to the technologies and infrastructures needed. By integrating European research regarding technologies, the project aims to: support identity and identification, interoperability of identity and identification concepts, ID-theft, privacy and security, and also profiling and forensic implications

The results, so far achieved by FIDIS cover integrated approaches to research, legal, socio-economic, usability and application requirements, and also a public architecture and specifications.

Although the scope of the project is on the information society, some delivers were made for eHealth context considering the state of the art in identity management systems and recent developments (D.317) and an application of the management method to interoperability within

eHealth (D4.9). The project made also a survey on eHealth identity management in several types of welfare states in Europe (D4.11), however Portugal was not characterized in this survey.

3.7 Liberty Alliance

The Liberty Alliance Project [38] is a global alliance of companies, non-profit and government organizations developing open standards for federated network identity, interoperable strong authentication and Web services. It started in 2001 with the specified purpose of "establish open standards, guidelines and best practices for identity management." The Liberty Alliance contributed on identity management from the federation specification, ID-FF, to OASIS, forming the foundation for SAML 2.0, the converged federation specification that is nowadays recognized by Liberty.

Liberty Federation was deployed in several organizations around the world. The liberty alliance solution allows the users to authenticate and sign-on to a network or domain and be able to access to multiple websites, in a federated approach, where user doesn't have to re-authenticate supporting privacy controls established by the user.

Liberty Alliance structure is formed by several groups, such as: Identity Assurance Expert Group, Identity Assurance Special Interest Group, Identity Theft Prevention Group, Strong Authentication Special Interest Group and others. The group that focuses on eHealth identity is Health Identity Management Special Interest Group, aiming to discuss privacy of networked health records as a whole, creating a forum for industry recommendations and action. It is recognized by Liberty Alliance that the challenges related to identity are not just about technology.

Liberty Solutions for Healthcare identified the following needs [61]: (1) *the support of 3 key elements of National Health Information Network (NHIN) interoperability:* Non-proprietary interoperable authentication of individuals and devices, record locator service to provide directory of records across all constituent sub-networks and enforcement mechanism to assure standards compliance by participating sub-networks; (2) *Make it much easier for patients, providers and payers to share results of authentication* (securely, in a controlled manner, easily) and (3) *enable easier, faster HIPAA and other "best practice" compliance* (access control, audit control, authorization control, entity authentication). The concept of federated identity [61] helps establish a virtual network of organizations and users through authentication and single sign-on across domains where identity information is kept in the organization domain, but can be linked together to be used between different domains, allowing healthcare providers, insurance companies, pharmacies, public health centers and even individuals to share information securely while protecting personal health information.

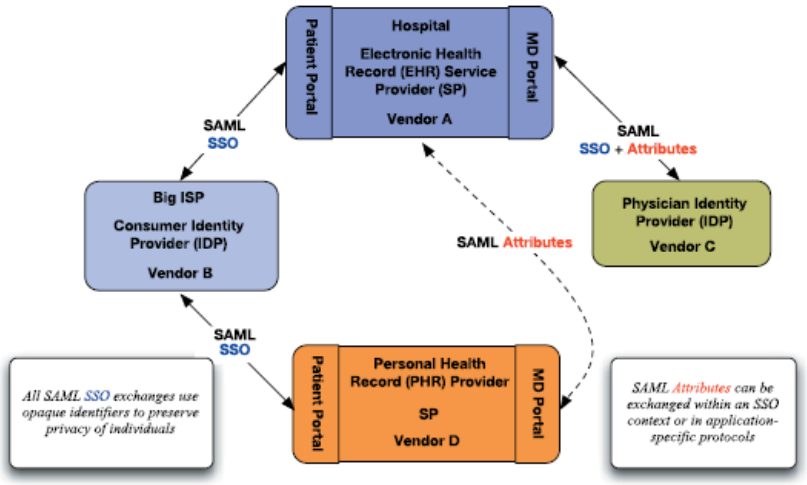

Figure 4 Liberty Alliance - standards-based federated Identity in eHealth context

Figure 4 Liberty Alliance - standards-based federated Identity in eHealth context, represents the workflow and methods used to establish relationship between parties (service and identity providers).

Some important implementation, with outcomes specifications of Liberty Alliance were: (1) Catalan Health Service E-Prescription Project, that connects medical doctors, hospitals, pharmacies and the Catalan Health services using authentication mechanisms based in an identity federation and SAML 2.0, (2) NHS (National Health Service) Connecting for Health, with Liberty Federation specification, to connect over 30.000 general practitioners in England to almost 300 hospitals and give patients access to their personal health and care information.

3.8 TAS ^{3}: Trusted Architecture for Securely Shared Services

TAS^{3} is another ICT co-funded research project in FP 7 (Comission, 2010b). The value of this research project rely on the management of privacy information typically generated over a human lifetime and therefore collected and stored in distributed locations and used in a multitude of business processes. The project started on January 2008 and will end on December 2011.

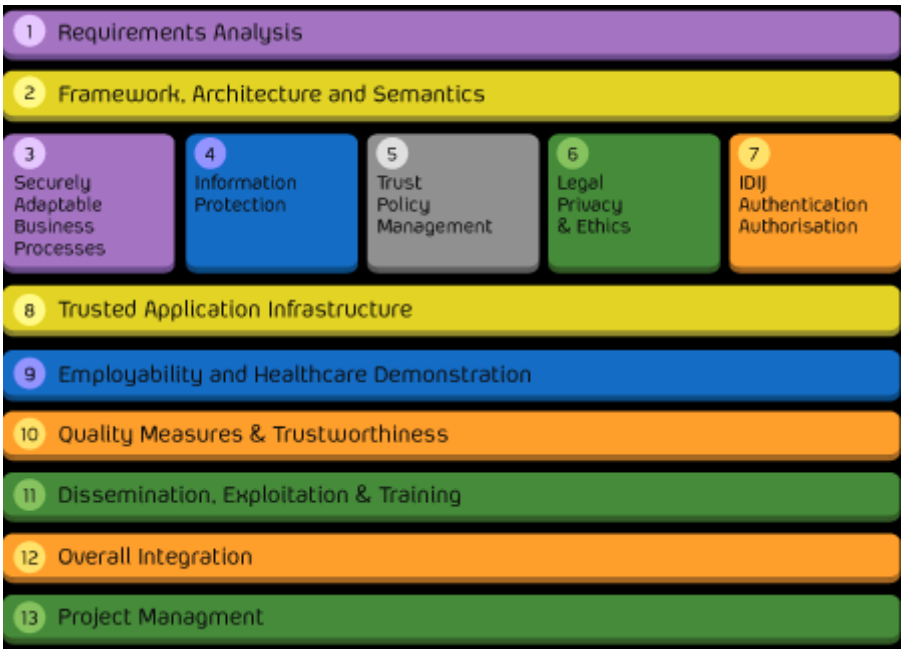

Figure 5 - TAS³ Work packages

TAS³ consider that trust and authorization policies are mostly defined specifically to their application and to the context in which they live. This creates an important barrier when the applications need to be interoperable in a cross-context solution. As the systems do not naturally support cross-context solutions and they are intrinsically non-interoperable, it increases the complexity weakness the deployment in cross context environment which might lead to decrease the trustworthiness of the resulting system [62].

TAS³ explore this problem, and proposes an architecture which is context independent, and share the following business and technical visions: (1) from the business perspective "*is that all parties involved should feel secure and consider the network to be trusted and TAS³ is to lay the trust & security foundation for a services economy based on personal identifiable data. This includes the design and use of a trust architecture through which on the one both the individual can self- manage his/her distributed personal information, while at the same time the usage of this data can facilitate new or enhanced user-center business processes*"[62], (2) from the technical perspective, the TAS³ integrated project "*provides a transparent framework in which process based services can securely process and depend on personal information, regardless from the context in which this information was collected. This requires, of course, that the context of the business process is compatible with the data protection policies and that the requester has the proper authorizations to process this information, but if the service provider meets all these conditions, he becomes* part of a trusted service network *that guarantees that a service requester is only able to use services from a service provider that have never before been possible*" [62].

The work packages includes a deliverable for the design of Identity Management, Authentication and Authorization Infrastructure (D7.1), that was open for public comments, feedback and review [63].

3.9 Open Standards

There has been several open standards developments mechanisms for identity management systems to interoperable web single-sign-on and user attributes exchange.

Some of the projects identified and produced specification for Internet identity frameworks such as SAML, OpenID, OAUTH, and for identity healthcare Cross-Enterprise Security and Privacy Authorization (XSPA) profile of WS-Trust for Healthcare.

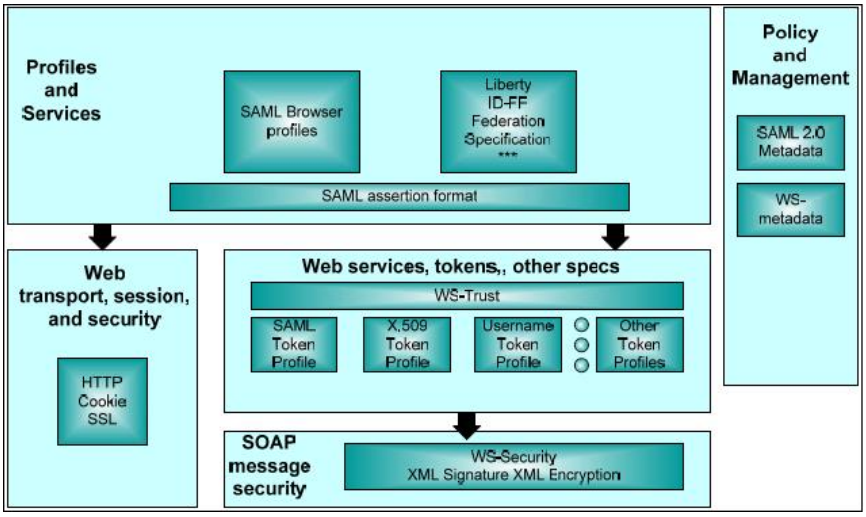

Figure 6 Open Standards

3.9.1 OpenID

OpenID [64] was created in 2005 by an open source community trying to solve a problem, like use an existing account to sign in to multiple websites, without needing to create new passwords. This question was not properly treated by others existing identity technologies. OpenID may be used by anyone, one can even become an OpenID Provider for free without having to register or be approved by any organization.

OpenID is a web registration and single sign-on protocol that lets users register and login to OpenID-enabled websites using their own choice of OpenID identifier. OpenID is a decentralized authentication protocol that makes it easy for people to sign up and access web accounts. The user can operate their own OpenID service, or can use the services of a third-party OpenID provider. OpenID is a community-developed open standard hosted by the non-profit OpenID Foundation.

One key advantage of OpenID is that it requires no client-side software and it works with any standard Internet browser.

3.9.2 OAuth

OAuth 2.0 [65] is the evolution of the OAuth protocol which was originally created in late 2006. OAuth1.0 provides a method for clients to access server resources on behalf of a resource

owner (such as a different client or an end-user). It also provides a process for end-users to authorize third-party access to their server resources without sharing their credentials (typically, a username and password pair), using user-agent redirections [66]. OAuth includes four roles working together to grant and provide access to protected resources - access restricted resources which require authentication to access [66]:

1. **resource owner** – an entity capable of granting access to a protected resource. When the resource owner is a person, it is referred to as an end user;
2. **resource server** - the server hosting the protected resource, capable of accepting and responding to protected resource requests using access tokens;
3. **client** - an application making protected resource requests on behalf of the resource owner and with its authorization;
4. **authorization server** - the server issuing access tokens to the client after successfully authenticating the resource owner and obtaining authorization.

3.9.3 SAML

The Security Assertion Markup Language (SAML), developed by the Security Services Technical Committee of OASIS, is an XML-based framework for communicating user authentication, entitlement, and attribute information. SAML is a flexible and extensible protocol designed to be used, and customized if necessary, by other standards. The Liberty Alliance, the Internet2 Shibboleth project, and the OASIS WebServices Security (WS-Security) committee have all adopted SAML as a technological underpinning for various purposes [67].

SAML 2.0 protocol facilitates exchange messages, requests and/or responses, between endpoints. Messages primarily have to exchange an identity assertion that includes authentication and attribute information. The endpoints are typically the Service Provider and the Identity Provider (IdP).

The SAML 2.0 can be used to conduct transactions in eHealth applications. Authentication may rely on the SAML 2.0 Web Browser Single Sign On (SSO) to facilitate end user authentication.

The benefits and advantages of SAML include [67]:

- Platform neutrality – SAML abstracts the security framework away from platform architectures and particular vendor implementations. Making security more independent of application logic is an important tenet of Service-Oriented Architecture.
- Loose coupling of directories – SAML does not require user information to be maintained and synchronized between directories.
- Improved online experience for end users – SAML enables single sign-on by allowing users to authenticate at an identity provider and then access service

providers without additional authentication. In addition, identity federation (linking of multiple identities) with SAML allows for a better-customized user experience at each service while promoting privacy.

- Reduced administrative costs for service providers – Using SAML to "reuse" a single act of authentication (such as logging in with a username and password) multiple times across multiple services can reduce the cost of maintaining account information. This burden is transferred to the identity provider.
- Risk transference – SAML can act to push responsibility for proper management of identities to the identity provider, which is more often compatible with its business model than that of a service provider.

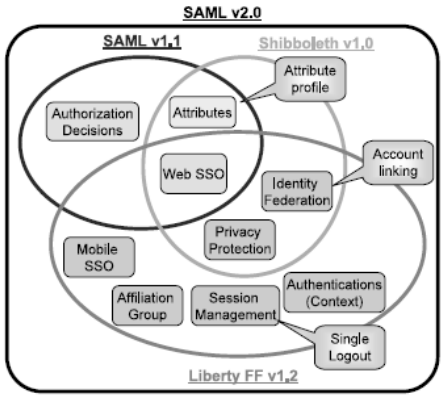

Figure 7 SAML v2.0: Relation of inclusion among SAMLv1.x, Shibboleth, and Liberty ID-FF1.2

In Figure 7, it is represented the relationship between SAML V2.0 and other protocols such as SAML V1.1, Shibboleth and Liberty ID-FF1.2 [68]. SAML is being used for web single sign on, attribute authentication, authorization, for securing web services and is defined by assertions, protocols, bindings, and profiles. Features like pseudonyms, identifier management, encryption, metadata, attribute profiles, session management, devices, privacy mechanisms and Identity provider discovery are some of the new features supported by version 2.0.

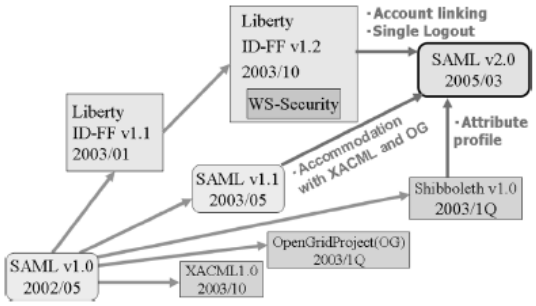

Figure 8 SAML 2.0

In Figure 8, shows the version update from SAML 1.0 to SAML 2.0 and how other protocols convergent to empower SAML 2.0 [68] with additional functionalities.

3.9.4 Liberty Alliance – Identity Federation Framework

Liberty Alliance has defined its Identity Federation Framework (ID-FF) [69] on the base provided by SAML V1.x, layering additional functionality. Recognizing the value of a single standard for federated Single Sign On, the Alliance submitted ID-FF V1.2 back into the OASIS Security Services Technical Committee as input for SAML V2.0, and the main objective was to use ID-FF in SAML V2.0 for identity federation pushing forward Liberty's Identity Web Services Framework (ID-WSF). Liberty ID-WSF is a platform for communicating identity information among web services developed and maintained by Liberty Alliance. The latest version of Liberty ID-WSF now uses SAML V2.0 assertions as the security token format for communicating authentication and authorization information amongst web service actors.

3.9.5 OASIS - WS-Trust

The WS-Trust is a OASIS standard specification, approved on March 2007 and it was authored by representatives of a number of companies. At the present the specification available is WS-Trust specification document v1.4, and WS-Trust is part of a WS-* specification standard that provides extensions to WS-Security. It was specifically defined to dealing with the issuing, renewing, and validating of security tokens, and with basic mechanisms to provide secure messaging between applications to construct trusted SOAP message exchanges[70].

Trust is the characteristic that one entity is willing to rely upon a second entity to execute a set of actions and/or to make set of assertions about a set of subjects and/or scopes. This trust is represented through the exchange and brokering of security tokens[71].

In the Healthcare environment a specification framework has been defined for Cross-Enterprise Security and Privacy Authorization (XSPA) profile of WS-Trust for Healthcare Version 1.0. This framework provides access control interoperability, useful in the healthcare environment. Interoperability is achieved using WS-Trust secure token request/response element to carry common semantics and vocabularies in exchanges [72]. Figure 9 Interactions as demonstrated RSA 2010 Oasis XSPA Interop provides detailed information during the information exchange between two healthcare organizations and is representative of the architecture demonstrated at the RSA 2010 Oasis XSPA interoperability demonstration (Interop) in March of 2010.

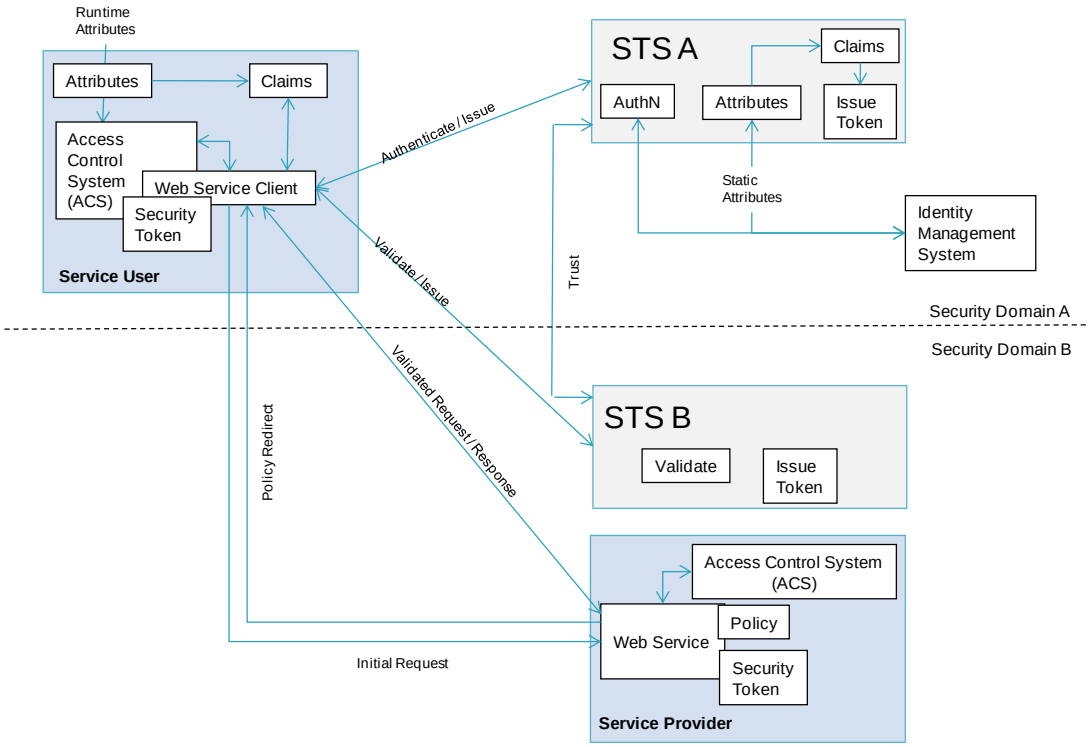

Figure 9 Interactions as demonstrated RSA 2010 Oasis XSPA Interop[1]

3.10 Shibboleth

The Shibboleth System [73] is a standard based open source software for web single sign-on across or within organizational boundaries. It allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner. Shibboleth is federated identity system and it takes the following advantages for being a federated identity system [73]:

- It delivers authoritative user attributes directly from the organization responsible for the credentials;
- Resource providers not longer need to manage accounts, plus access is broadened;
- User data is protected. Storage at a single, hardened location and stringent release policies minimize the chance of privacy violation;
- The user experience is improved, with no special software, no proxies, and no configuration required. Single sign-on is possible.

This provides Shibboleth two types of value:

---

1 Interactions as demonstrated RSA 2010 Oasis XSPA Interop, in specification document , OASIS standard "*Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of WS-Trust for Healthcare Version 1.0*"

- Single Sign on – allow the use of a single password, along with the resulting improvements in security;
- Protection against unnecessary disclosure of personal attributes, resulting in preservation of privacy

Federated identity supplies user information to applications offered by different organizations allowing for single sign-on, one identity for common access, and provisioning of authoritative data. When a user wants to access a controlled resource, a set of attributes is collected dynamically and delivered to the application. Based on this real-time provisioning, the application can make a decision to grant or reject access, or can customize the application for the user [73].

Shibboleth supports several profiles and protocols. There are some successful initiatives using Shibboleth, namely Authentication and Authorization Infrastructure (AAI) [74] already in use in several universities, for example in OPorto University. The use of AAI with associated with STORK services allow the authentication and authorization of students to be done across borders and the exchange of personal attributes in a federated way for authentication and authorization.

In the eHealth domain, a test with Shibboleth and a eID card was made in Belgium [75]. The test described the different steps when a new partner joins the federation of the eHealth IdP (Identity Provider) and the SPs (Service Provider) of its partners. There were no intention on this test the need for a real protected application or real authentication scenario's, the main purpose was to test that any belgian citizen with in his possession of an eid-card or a username/password/token provided by Fedict [76] (Fedict is a Federal Public Service of Belgium) will be able to complete the testcase, allowing the testing of the communication between the partner's SP and the eHealth IDP in a first phase.

3.11 IdM characterization in Health

FIDIS project produced a delivery result *D4.11: eHealth identity management in several types of welfare states in Europe* [77]. This deliverable describes eHealth and the use of (health data from) electronic health records and cards in several states in Europe. A questionnaire was applied to several issues addressed are patient identifiers, access to medical data, use of medical data for profiling purposes. A characterization was made for several welfare states in Europe. Since Portugal was not included in the participants States, we applied the same questionnaire to national authorities, and the results and discussion of the results are presented in this subsection and a briefly comparison with other welfare states in Europe is made.

3.11.1 FIDIS IDM characterization in eHealth

FIDIS research was comparative. It was selected a sample from Northern, Southern, Western and Eastern countries in Europe, in order to get a cross-sectional view of developments in Europe.

The result of this study was explorative in nature. It was considered as a study limitation that the scope of countries was too limited to provide an exhaustive representation of EU states. In some preliminary operational questions, regarding eHealth in general two questions were applied:

1. What is eHealth, the electronic health record and electronic health cards?
2. What are the narratives in the debate on eHealth (and especially in relation to the use (the collection, saving and processing) of health/medical data)?

In eHealth tools in specific:

1. What is the state of art of deployment and implementation of eHealth tools in the questioned countries?

In profiling:

1. What about the collection of medical data?
2. What about saving medical data?
3. What about using medical data?
4. What are the benefits and risks of electronic health records and cards in relation to profiling practices?

One of the main results presented was the" diversity in the deployment and use of the electronic health records and electronic health cards. Variety can be related to specific necessities in the institutional fields (e.g. primary or secondary line of care, centralized or decentralized systems)."

Even regarding simplified communications between healthcare professionals and between healthcare professionals and patients, and as well as in the light of cost-effective and efficient health care delivery, "*it cannot be denied that eHealth tools (will) facilitate profiling practices to a bigger circle of parties."*

It was considered that "In general terms too little attention is being paid to the particular nature of health care, as a sociological, cultural, political and economic construct. Health care is not like other industries; moreover it is directly related to welfare issues. Universal and equity access, social justice and quality of the healthcare systems are aspects which must be taken into account before designing and implementing eHealth."

Additionally it is also considered that "Socio-technical choices in health care have to be made within the specific normative, regulative and cultural context of regions or nations."

4 PROPOSED IdM MODEL

4.1 Introduction

The main technical and organizational challenges in identity management systems are promoting efficiency, availability, cross-context interoperability, trusted and reliable mechanism for legal issues and demand for technological solutions providing security and privacy, matching with legal aspects and policies with significant impact in the eHealth context.

This chapter describes a new model and is structured in the following sections: description of the architecture chosen for the model, followed by the description of the major blocks that make up the model and its function and finally the description of each block composition and relationship with different actors.

4.2 The parties involved

The National Health Service (NHS) in Portugal is composed of a set of institutions and services, in the dependence on the Health Ministry, whose mission is to ensure health care access to all citizens within the limits of available human, technical and financial resources[78].

The NHS also includes private health organizations and healthcare professionals serving in the private sector, that have been awarded contracts or agreements, which guarantee the right of access for users in a manner similar to those offered by the NHS.

The parties involved in health care providing and for which the model should recognize and respond are therefore: the patient, the healthcare professionals and the organizations where healthcare is provided. Next sections describe in detailed each of the involved parties and their main characteristics that must be recognized by the identity model.

4.2.1 Patients

Patients rights to health protection are enshrined in the Constitution of the Portuguese Republic based on core values such as human dignity, equity, ethics and solidarity.

The beneficiaries of the NHS are: (i) Portuguese citizens, or (ii) national citizens of the Member States of the European Union under the Community rules, or (iii) foreign nationals residing in Portugal, subject to reciprocity, and stateless persons residing in Portugal.

Patients Rights

According to the Portuguese law, *Lei Bases da Saúde* [78], patients covered by the NHS have following rights: (a) The patient is entitled to be treated with respect for human dignity; (b) The patient has the right to respect for their cultural beliefs, philosophical and religious; (c) The patient has the right to receive appropriate care to their state of health in the context of preventive, curative, rehabilitative and terminals;(d) The patient has the right to a continuum of care (Tertiary care); (e) The patient is entitled to be informed about existing health services, skills and levels of care; (f) The patient is entitled to be informed about his health situation; (g) The patient has the right to obtain a second opinion on their health situation; (h) The patient is entitled to give or refuse consent before any medical procedure or participation in research or clinical training;(i) The patient has the right to confidentiality of all clinical information and personal details which concern him; (j) The patient has the right to access data recorded in his medical file; (l) The patient has the right to privacy in any medical procedure; (m) The patient is entitled, personally or through their representative, to make suggestions and complaints;(n) Choose the service and healthcare professionals, as existing resources and in accordance with the rules of organization;

Patients' duties

According to the law, patients duties are: (a) Respect the rights of other patients; (b) Observe the rules of organization and operation of services; (c) Collaborate with healthcare professionals regarding your own situation; (d) Use the health services in accordance with the established rules; (d) Pay the costs arising from the provision of health care, when appropriate; (e) Constitute entities that collaborate with the health system, particularly in the form of associations for the promotion and protection of health.

Patient characterization

Patients can then be characterized by different attributes, in the universe of national health system to which they belong. The set of information about the patient may be related with: (i) civil identification, which characterizes and qualifies the patient as a citizen (National, Foreign resident, or European citizen); (ii) the health organization service delivery and the professionals that are recognized to delivery health care according to the patient right to choose the health organization and healthcare professionals, given the existing resources and in accordance with the organization rules.; (iii) the subsystems that provide the reimbursement for the provision of health care; (iv) the benefits they are entitled, either by disease status, eg chronically illness like diabetes, or by their social status, eg pensioners whose total annual income is equal to or less than fourteen times the national minimum wage.

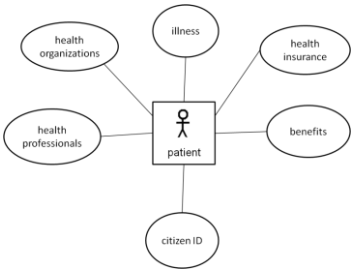

Figure 10 Patient characterization

Patient attributes in health context

The proposed model links the patient with his characterization in the health context. The identification of the patient attributes needed by the characterization given are related with: (i) their civil identification: name, birth date, birthplace and nationality, and in addition home address and patient national identifier (PNI); (ii) organization health service delivery and the professionals that are recognized to delivery health care – Health organization identification and professionals ID, such as chambers ID number; (iii) insurance delivered by a provider, ID number and validity of the insurance and if applicable the level of insurance agreed; (iv) benefits, special arrangements for reimbursement of medicines, tax moderator exemption access to health services, other special situations of reimbursement provided by law; (v) some of the benefits are only achieved on illness state, and depending on the illness program, some of the reimbursement are provided to the patient. Other applications that can contribute with relevant attributes are for example organs donation program, which is an optout system that identifies a patient not to be an organs donator.

Patient ID in health context

The patient ID is established by a national number that is assigned to the patient. Presently, the patient ID registration process and respective card issue is changing from a national patient card to a national citizen ID card that includes the national patient identifier.

The patient is registered directly in NHS when he registers for Citizen ID Card. However, as Portugal is moving towards the Citizen ID card, in the Health context, the patient can still register in a primary health care centre, and the patient have to present and proof evidence on his civil identification, social security card or other insurance card and some document that gives the proof of his home address. Then, a search is done in national patient registry, called RNU. If the registration already exists, based on patient name, birthdate and home address, there is no need to create a new one. If no registration is found, the information system requests for a national patient identifier number which is assigned to the new patient.

Nowadays if the patient is free of user fees in health services access, or have special arrangements for reimbursement of medicines, the patient must proof that fact with documents that give evidence that he can have those benefits. After this registration process is done on the primary health center, that patient is given a paper document that is needed for the registration process to get the citizen ID card issued.

4.2.2 Health Professionals

A professional class is characterized by the homogeneity of the work performed by the knowledge required for such tasks and preferably the identity certificate for the exercise thereof. The professional class is thus a group within society, specific, defined by specialized knowledge and task performance. Health professionals are grouped in professional classes. Considering the healthcare professionals mobility directive is established by the European Directive 2005/36/CE, for this study it is considered as examples the follow healthcare professionals classes: specialized doctor, nurses responsible for general care, dental practitioner, as specialized dental practitioner, and pharmacist

4.2.2.1 General overview on healthcare professional recognition

For the automatic qualification recognition of each health care professional, is first needed to be recognized evidence of their formal qualifications provided universities. Then for physician practice is also needed a registration process in the respective chamber, that represents the professional class [79].

According to HPRO the detailed qualification process can be represented as in Figure 11.

Tree different phases are considered: (1) University as a graduated provider, (2) Right to practice provider management, as class chamber, (3) Health class professional card/document.

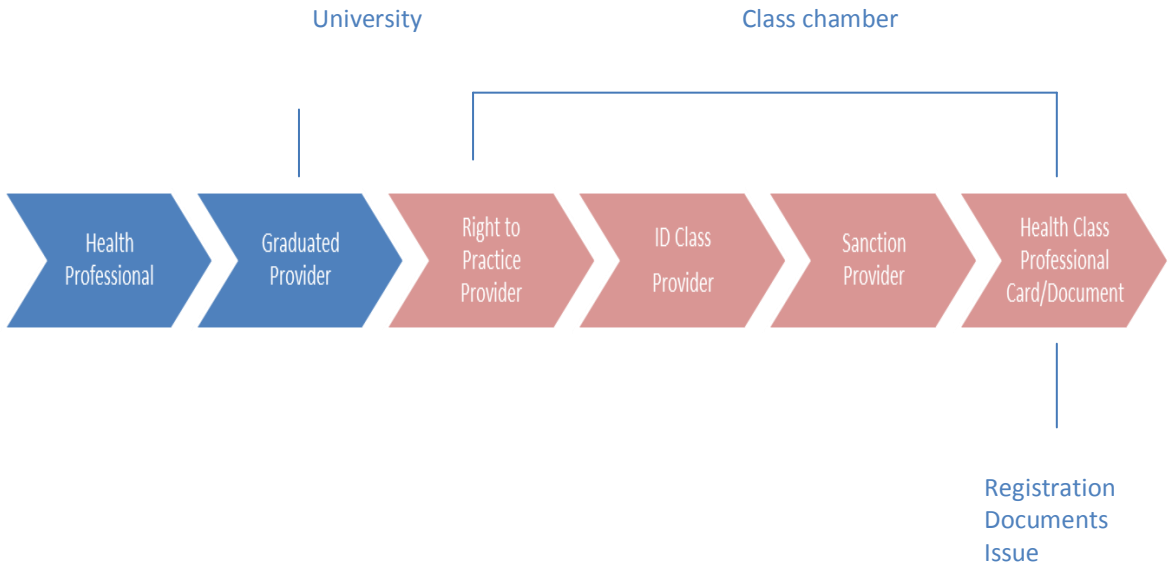

Figure 11 HPRO - Qualification process detail

In Portugal there are a few class chambers that provide the registration process to authorize practice for healthcare professionals' classes. Most of them are represented by associations and by ACSS – Administração Central do Sistema de Saúde, if the class is not represented by any association.

Table 2. Number of professional in public NHS

	Physicians		Nurses		Other Health care professionals		Other professionals	
	n	(%)	n	(%)	n	(%)	n	(%)
Public PHC	7.062	29%	7.807	20%	995	10%	10.891	23%
Public Hospitals	17.153	71%	31.245	80%	9.440	90%	36.432	77%
Total	**24.215**	**100%**	**39.052**	**100%**	**10.435**	**100%**	**47.323**	100%

According to the national report on resources and production from the year 2009 of NHS in Portugal [80], the number of physicians in primary health care (PHC) centre are 6825, and 6065 of those have an specialization practice, representing 88,9% practice physicians in primary care. Therefore specialization practice is a qualification attribute for physicians.

Médicos		Enfermeiros		Técnicos de Diagnóstico e Terapêutica	
Total	**6825**	**Total**	**7631**	Fisioterapeutas	139
Clínicos Gerais (não especialistas)	760	Cuidados Gerais	6624	Hig.Orais	110
Especialistas	6065	Especialistas	1007	Téc. Radiologia	159
Medicina Geral e Familiar	5567	Saúde Infantil e Pediátrica	199	Tec.Anál. Cl./ Saúde Pública	46
Dermatologia	15	Saúde Materna e Obstetrícia	210	Tec. Hig. e Saúde Ambiental	395
Estomatologia	11	Enfermagem Médico-Cirúrgica	22	Outro Pessoal Técnico	122
Ginecologia/Obstetrícia	26	Saúde Mental e Psiquiátrica	46	**Técnicos Superiores**	
Medicina Dentária	23	Reabilitação	108		
Oftalmologia	4	**Pessoal Técnico Superior de Saúde**		Tec. Serviço Social	252
Otorrinolaringologia	22			Outros Técnicos Superiores	93
Pediatria	27	Ramo Engenheiria	4	**Outros Profissionais**	
Pneumologia	2	Ramo de	14		
Psiquiatria	3	Ramo Nutrição	73	Administrativo	6319
Saúde Pública	316	Ramo Psicologia	175	Serviços Gerais e Auxiliar	3804
Outras especialidades médicas	49	Outros Técnicos	29	Outro Pessoal	161

Figure 12 Professional in primary healthcare centres – 2009

4.2.2.2 Details on the qualified authorities

A qualified authority is the entity responsible for issuing the right to practice for healthcare professions. According to the European Directive 2005/36/EC: A qualified authority is « *any authority or body empowered by a Member State specifically to issue or receive training diplomas and other documents or information and to receive the applications, and take the decisions, referred to in this Directive".*

To practice medicine, physicians must register in *Ordem dos Médicos* (OM), in accordance with the statutes of OM [43]. OM is the organization to which the Portuguese government delegated the

task for the accreditation and certification of specialized training for medical graduates ensuring the quality of medicine, and the accuracy requirement of medical training and thereby is in part responsible for the Portuguese health care quality.

The duration of the specialized training is determined by the specialist colleges of medicine and varies according to discipline, for example, internal medicine and neurosurgery take six years, whereas anesthesiology takes four years. Specialists must be skilled in the diagnostic and treatment procedures of their own specialty and must be proficient in related techniques. After recognition of their aptitude, they can apply for a hospital position or go on to clinical practice.

Some of the existing authority sources in Portugal are represented by:

- ***Ordem dos Enfermeiros*** (OE) is a public association representative of registered nurses with academic and legally professional qualifications required for exercising of the nurse profession[44].
- ***Ordem dos Farmacêuticos*** (OF) is the public association that represents and encompasses graduates in Pharmacy or Pharmaceutical Sciences in the profession or pharmaceutical practice acts themselves [81]. The use of the title of pharmacist and practice of pharmacy profession depend on their own acts of registration by such member.
- ***Other health care professionals,*** for instance oral health care was provided by stomatologists who undertook three years' specialist training after their medical degree. Another nonmedical grade exists, that of odontologist. This professional class was introduced by the Government at a time when there was a severe shortage of dentists, but it has been replaced by the degree in dental medicine awarded by higher education institutions. There are also several allied medical professional degrees being offered, covering 18 specializations (such as physiotherapy and radiology).

The registration processes for healthcare professionals and the list of competent authorities is presented in table 3. The issuing of the respective documents completes the processes of healthcare professional's registration. The description of these processes shows also the methodology used by each professional class in the registration process.

Table 3 Health professionals careers and registration source authority

Professional Class	Qualification	Degree	Law and regulation	Activity	Source Authority
Physician	Physician	Yes	DL 282/77, July 5th		Ordem dos médicos
Nurse	Nurse	Yes	DL 111/2009		Ordem dos enfermeiros
Dentist	Dentist	Yes	DL 110/91, August 29th		Ordem dos médicos dentistas
Odontologist	Odontologist	Yes			Ordem dos médicos dentistas
Health technician	Heath Superior Technician	Yes	DL 414/91, October 22nd; DL 501/99, November 29th	Sanitary engineering	Ordem dos engenheiros
				Pharmacy	Ordem dos farmaceuticos
				Hospital physics	NA
				Genetics	Ordem dos farmaceuticos (in case Pharmacy degree)
				Laboratory	Ordem dos farmaceuticos (in case Pharmacy degree)
				Nutrition	NA
				Veterinary	Ordem dos veterinários
				Clinical psychology	Ordem dos psicologos
Diagnostics and therapeutics technician	Diagnostics and therapeutics technician	Yes	DL 320/99, August 11th	1. Technical of clinical analysis and public health; 2. Technical pathology, cytology and thanatological; 3. Cardiology Technician; 4. Neurophysiology Technician; 5. Nuclear Medicine Technician; 6. Radiographer; 7. Radiotherapy Technician; 8. Dietician 9. Technical audiology; 10. Speech Therapist; 11. Physiotherapist; 12. Occupational therapist; 13. Orthopedics; 14. Orthoptists; 15. Dental technician; 16. Pharmacy Technician; 17. Oral Hygienist; 18. Environmental Health Technician	ACSS
Technician	Superior Technician	Yes		NA	Qualification (University)
Technical Assistant	Technical Assistant (former Administrative Assistant)	No		NA	NA
Operational Assistant	Operational Assistant (former auxiliary administrative)	No		NA	NA
Specialist and informatics technician	Specialist and informatics technician	Yes/No		NA	Qualification (University)
Other carears		Yes	DL 121/2000	Scientific research	NA
				Inspection	NA
				Kindergarten, primary school teacher	NA

Some professional classes can have their source authorities for professional qualification with universities. However there are professional classes who have no professional association that

regulates their activity, in these cases the source of true is the universities where they were graduated. Other healthcare professionals are only identified locally without any professional association or qualification assigned.

4.2.3 Health organizations – Entities

The registration of health care providers (HCP) is through *Entidade Reguladora da Saúde* (ERS) which is the regulatory authority for health providers. Health care providers must be registered to perform their activity [82].

Health Providers are subject to mandatory registration by the ERS. The relevant information for a correct identification of health providers, includes: a) Complete identification of the entity; b) Constitution of the entity; c) Identification of the shareholders of the social entity; d) Bodies of social organization; e) Identification of the various entities held or coordinated by the organization; f) Identification of technical managers of establishments and its services; g) management contracts, agreements and conventions, each entity and its establishments are involved. Individuals are exempt of the elements contained in paragraphs b), c), d) and f) above.

4.2.3.1 Organization of the entities in the health system

According to the organizational structure of the Ministry of Health, represented in Figure 13, the Ministry of Health is comprised of several institutions, each under the direct administration of the State (led by the Ministry of Health, through a hierarchical relationship), others under indirect state administration, some having status as a public company and an advisory body. The Health Regulatory Authority (ERS) in the independent in the exercise of their functions.

Recently, the public administration is being reformed, and currently, the NHS is restructuring the primary care services by implementing the USFs, which are primary health care centers with a small team, with a few GPs, and nurses and the support of administrative professionals, usually covering a population between 5000 and 14 000 patients. The USF team, have functional and technical autonomy and a payment system sensitive to performance that reward productivity, accessibility and quality. Their main goal is to maintain and improve the health status of people covered by them through general health care delivery in a personalized, accessible and continued way.

4.2.3.2 The role and relationship between entities

The role and relationship of each entity is very important for a good organization of National Health Service. Each of the health entities are represented in the organizational structure of the Health Ministry has its mission and competencies, and the main NHS entities and services available are briefly described.

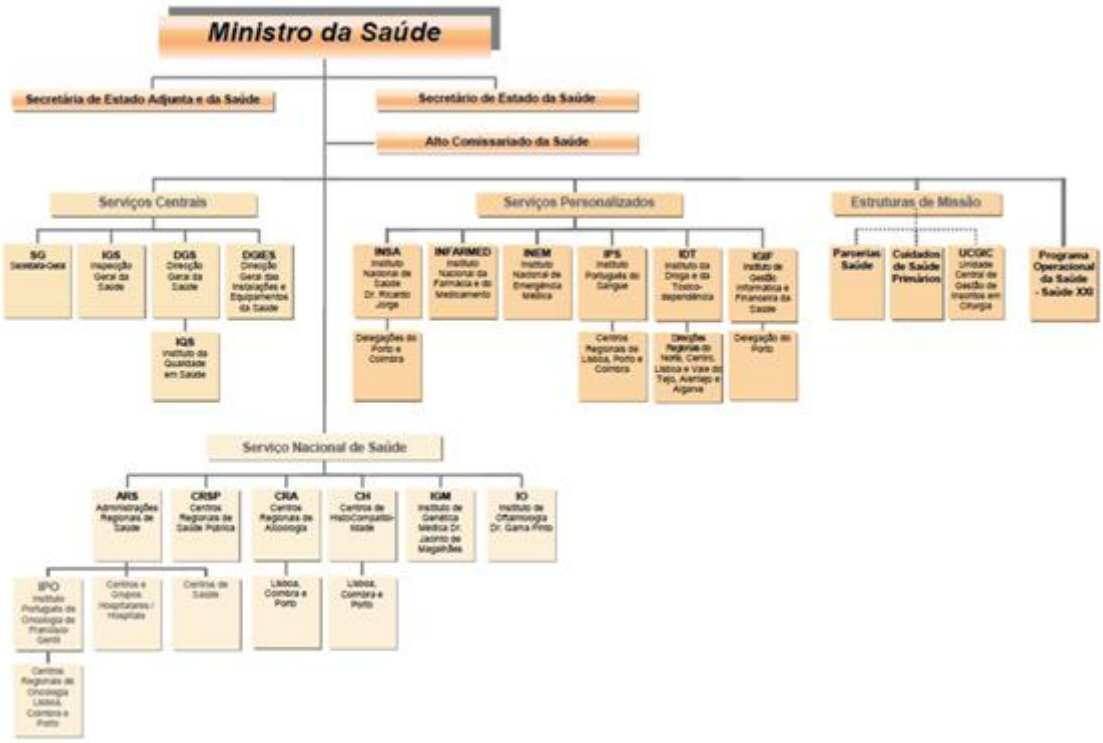

Figure 13 Health entities organizational chart

Source: Portal da Saúde

The General Secretariat of Health - *Secretaria-Geral* (SG)

The SG is responsible to provide a technical and administrative support to the other departments of the Ministry, coordinating their work and providing assistance to staff within various government offices. The SG gives support to other entities, services and human resources not integrated within the NHS, concerning internal resources, legal advice, information and public relations.

The General Directorate of Health - *Direcção–Geral da Saúde* (DGS)

The General Directorate of Health (DGS)[83] is the central service of the Ministry of Health, part of the direct administration of the state, endowed with administrative autonomy. The DGS plans, regulates, directs, coordinates and supervises all health promotion, disease prevention and health care activities, institutions and services, whether or not they are integrated in the NHS. DGS is responsible for: (a) Guide and develop public health programs, improved health care delivery and continuous improvement of clinical quality and organizational; (b) Coordinate and ensure surveillance at the national level, in context with other EU member states and international organizations; (c) Develop and disseminate health statistics; (d) Promote technical studies on health care; (e) Develop technical cooperation activities; (f) Support the exercise of the powers of the

National Health Authority; (g) Coordinate System for Public Health Emergency; (h) Monitor the Service Center's National Health Service

The Authority for Blood and Transplantation Services - *Autoridade para os Serviços de Sangue e Transplantação* (ASST)

The ASST[84] has the mission to monitor the quality and safety of organ donation, collect, processing, storage and distribution of human blood and blood components as well as ensuring the quality of the donation, collection, handling, preservation, storage and distribution organs, tissues and cells of human origin.

Central Administration of the Health System - *Administração Central do Sistema de Saúde* (ACSS)

The ACSS [85] is a central service under the State's indirect administration, and is in charge of the financial and human resources management , facilities and equipment, systems and information technology (IT) of the NHS. It is also responsible for the definition of policy, regulation and planning of health, along with the Regional Health Administrations (RHA), namely in the area of health service contracting.

The National Authority on Drugs and Health Products - *Autoridade Nacional do Medicamento e Produtos de Saúde* (INFARMED)

INFARMED[86] has the mission of regulating and supervising the areas of drugs, medical devices,cosmetics and body care, according to the highest standards of public health protection, and ensure access of healthcare professionals and citizens to drugs, devices medical, cosmetic and body hygiene, quality, effective and safe.

The National Institute for Medical Emergencies - *Instituto Nacional de Emergência Médica* (INEM)

National Institute for Medical Emergencies (INEM)[87] is the organization of the Ministry of Health responsible for coordinating the operation, in mainland Portugal, of an Integrated Emergency Medical, to ensure the prompt and correct provision of health care to victims of accidents or sudden illness. The provision of aid at the scene, assist the transportation of victims to the hospital and appropriate coordination between the various actors of the system, are the main tasks of the INEM.

Portuguese Blood Institute - Instituto Português do Sangue (IPS)

The IPS[88] regulates, at a national level, the pharmaceuticals related to transfusions and ensure the availability and accessibility of blood and quality and safety of blood components. The IPS is responsible for the national blood donator card.

Figure 14 National blood donator card

This card is issued to every citizen that has donated blood, at least for one time. The use of this card is regulated by portaria 790/2001. Accordingly with law 790/2001, due to the increasing complexity and demands for quality and safety of blood, it was considered necessary to adopt and implement more efficient technological solutions. The national blood donor card has memory, with chip and magnetic stripe, where it is possible to register and allow reliable access to donor's history.

National Institute of Drug Addiction - Instituto da Droga e da Toxicodepência (IDT)

The IDT[89] promotes the reduction of both legal and illegal drugs consumption, as well as the decrease in drug addictions. Its vision is to be a national reference entity, with international recognition, for intervention in addictive behaviors.

National Institute of Health, Dr Ricardo Jorge - *Instituto Nacional de Saúde Dr Ricardo Jorge* (INSA)

The National Health Institute Dr. Ricardo Jorge (INSA)[90] is a public organization within indirect State administration under the Ministry of Health, autonomous in terms of scientific, technical, administrative, financial and own assets.

INSA develops a triple mission as State laboratory in the health sector, the national reference laboratory and observatory for national health. It aims to increase gains in the public health sector, along with health monitoring and epidemiological surveillance, either in the field of laboratorial or genetic medicine. It is responsible for conducting, coordinating and promoting health research at the Ministry of Health. It should also produce evidence for policy and action in public health.

Regional Health Administrations (RHAs)

The NHS, has a strong regional structure since 1993, with five regional health administrations: North, Centre, Lisbon and Vale do Tejo, Alentejo and the Algarve. Each region has health administration board, managing regional health services.

The RHAs are responsible for the regional implementation of national health policy objectives and coordinating all levels of health care mainly in primary health care, working in accordance with principles and directives issued in regional plans and by the Ministry of Health.

4.2.3.3 The relationship between entities, healthcare professionals and patients

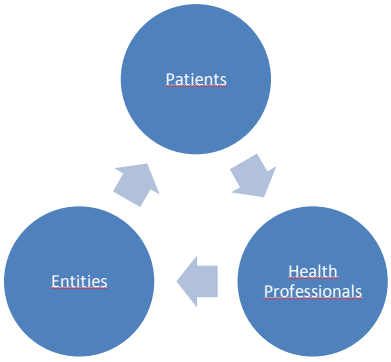

Figure 15 Relationship between entities, healthcare professionals and patients

Patients, healthcare professionals and entities are all related with each other, since healthcare professional usually have roles in health entities such as hospital, primary health care or private general practice. Conducted roles can also be assigned between health care professionals and patients.

4.3 Applications

Some of the eHealth application functionalities and access control that can take advantage of an interoperable IdM infrastructure are: electronic health record access under patient control; send a referral notice to a specialist; send discharge summaries from a public hospital to primary health care; electronic prescription and dispensation. A complete picture of the actions taken by software applications is a crucial element for a realistic risk assessment. Applications should therefore be classified by the degree of sensitivity of the data they carry and the actions they perform with data, and this must also be taken into consideration to evaluate the security impact that might arise in the presence of false or compromised identity assertions. Moreover the existence of a pre-defined classification of required assurance levels for applications provides the means to impose a minimum threshold for the assurance level requirements of the authentication mechanism employed to validate a certain identity. This means that the authentication mechanisms used to validate a certain

identity must be at least compliant with a minimum established application security threshold, in order to be possible to use that application with that identity. The authentication assurance level and the credential types employed to validate a certain identity thus depend on a pre-established applications security assurance level classification for a certain administration domain.

4.4 Identity management system requirements

Emerging from technical models trend for user-centric identity management, the main requirements are:

(1) enabling patients to give informed consent on disclosure of personal information;
(2) allowing the patient to quickly determine what information can be revealed to which parties and for what purposes,
(3) determine how trustworthy those parties are and how they will handle the information;
(4) what the consequences of sharing personal information
(5) The patient must be empowered to give or revokes consent to others access his personal health information.

The IdM system may be an opt-in and opt-out system. In the op-tout model the patients are included by default within the system, and to leave it they have to give informed choice. This requires that patients should be well informed before the system implementation [91]. Op-tin is fairer, because an informed patient choice is given and there is no doubt about patient's intention on being registered in the system. The proposed IdMS should be optin for patients and healthcare professionals consent for attributes exchange and minimal information save should also be considered. The defined laws of identity are also important and the proposed IdMS should take them into account.

The requirement of not having an identity management system, that centralize every information about users (patient and healthcare professionals) is important because the digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship. – Only those parties authorized to access the data, because they are justifiably required to do so, are granted access. This is in sequence of minimal disclosure and the "need to know".

4.5 Proposed architecture for the identity model

The identity management model proposed is a user-centric identity management infrastructure.

The proposed architecture for the identity model is represented by four main components. For each component an explanation of the proposed cross-context identity management service in eHealth is made. There is the concept of Identity Provider (IdP) and Service Provider (SP) models characterized by access authentication and authorization in access to resources and finally the concept of monitoring and auditing system.

The IdP is a central authority acting as provider of the identity of citizen and professional qualification. SP provides applications, webservices or secure attribute exchange applications recognized by the identity management system, for example between local registered applications and central registered applications. For service providers, delivering resources such as applications, information, web services, and security classification information should be done, and the authentication mechanisms used should be defined according to the security classification need.

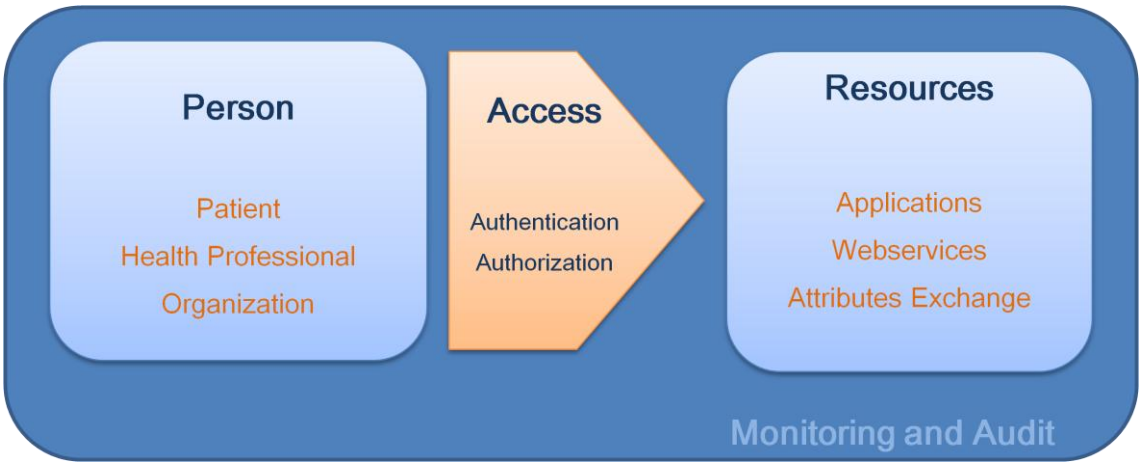

Figure 16 Identity model components

This user-centric identity management model allows the user to quickly determine what information can be revealed to which parties and for what purposes, determine how trustworthy those parties are and how they will handle the information, and to be aware of the consequences of sharing their information. This model enables users to give informed consent on the disclosure of personal information.

In a user-centric identity management, it is considered that the user can be profiled, which is possible for a patient or a healthcare professional, working on public or private organization. User-centric models put in the centre of interest the user and, give user empowerment, in this case over personal information. This means that when the user is a patient, the patient should be allowed to influence or even specify which information should be forwarded or be revealed to a particular service provider. This is in compliance with legal aspects, establishing user consent in releasing personal information between different service providers. The patient with the electronic consent

will be the intermediate for the authorization of personal data interoperability into different applications, delivered by the same or different service providers. The health system may have several service providers, as it was seen before, and the SP may ask for user attributes when information is need on a "*need know*" model.

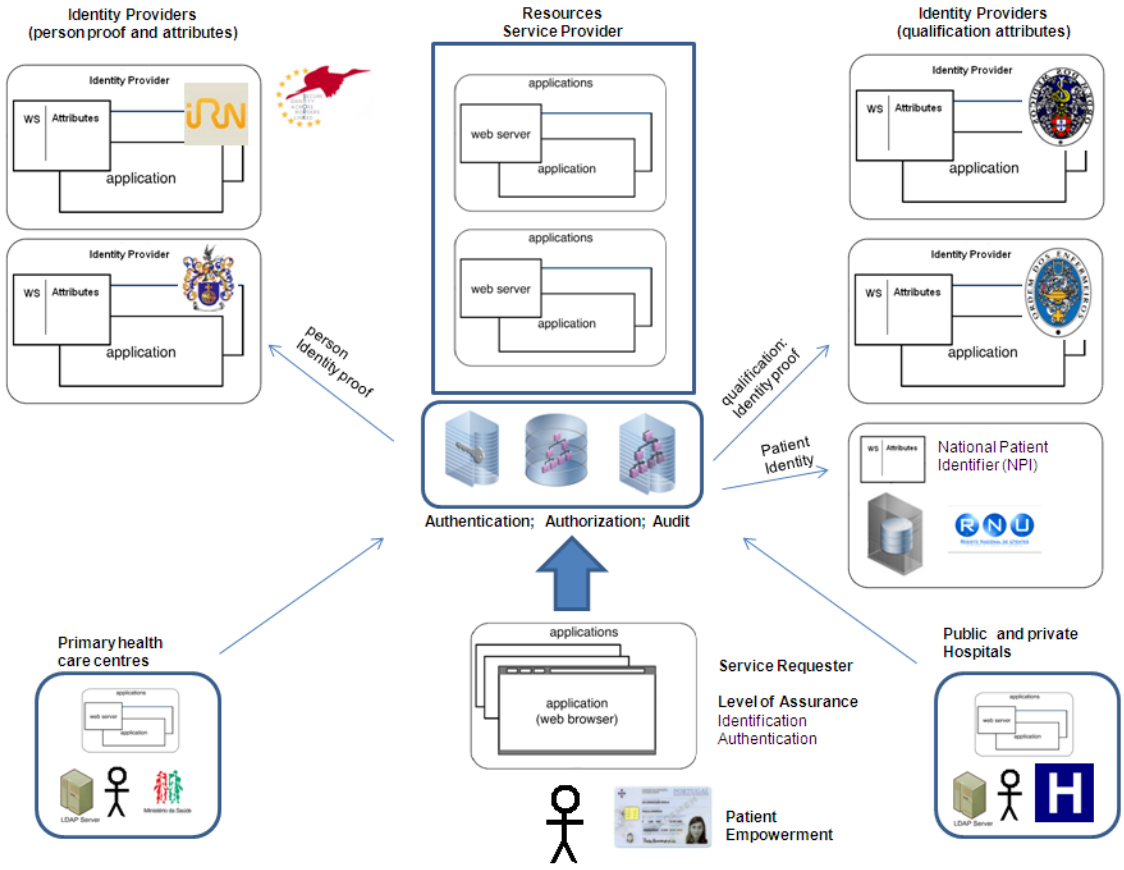

Figure 17. Source Authorities and Identity Providers

4.5.1 Users and Identity Providers

The IdM model must have a service provision based on the initial identification of the citizen and then for health care professionals on the professional qualification delivered by the source authorities. Then for services registered by service providers, and for the established roles, the patient should be allowed to subscribe services, and customize the utilization options available. The IdMS has three phases on service provisioning registration process represented in Figure 18

Figure 18 IdM phases on service provision

Description is made on authoritative sources regarding the service identification and procedures for roles to be implemented for user registration and service subscription process. Finally for privacy assurance, the meaning and the importance of pseudonymisation options are discussed for patient empowerment in the eHealth IdM model.

4.5.1.1 Authoritative Sources

A patient or healthcare professional identity is distributed throughout many systems and therefore have multiple identifiers such as: login ID, patient identifier number, professional ID, social security number, national ID, blood donator, email address, etc., which are unique within their own systems contexts, and usually systems store the identifiers from other identity systems.

Usually attributes have to be verified and validated on individuals by authoritative sources, known as attribute authorities. Identity is verified and validated by sources of identity, called identity provider(IdP) usually associated with a unique identifier, and all service providers, SPs will identify a specific user based on the same unique identifier from the common name space. The associated authentication token will normally be a public key certificate.

There is the concept of the IdP, which is a central authority acting as provider of the identity. For national citizens there is a Identity Provider called *Instituto dos Registo e Notariado* (IRN) [92]. When it is a foreigners citizen, with legal residence in Portugal, their identity is provided by *Serviço de Estrangeiros e Fronteiras* called SEF [93] which is the Office for Foreigners and Borders. Other European citizens identity is provided in the framework of the STORK [54] that defines the identity interoperability with other member states. According to the attribute of nationality, the source IdP organizations responsible for verification and validation are different.

Other IdP, responsible for managing attributes such as qualifications, benefits, and others may be also checked by the IdM System. Thus different authoritative sources are usually responsible for assigning different attributes to individuals and may remove, suspend or achieved attributes as well as assign them. The verification should be in real time, for a "Hit" or "no hit" in source authority, when the user claims to have an attribute value.

For example, if we consider Ordem dos Médicos (OM), the physician chamber, if for some reason the physician activity it's suspended, it is clear that OM is the authoritative source of physician practice status attribute. We can consider that OM keeps a register and manage the life cycle of the identities attributes related to physician, being responsible for registration attributes and to validate and verification of the attributes requests.

It is important to assure that the identity provider should only be responsible to assert a user's attributes, if the assert attributes are the ones they are authoritative for. For example, nurse practice qualification should be asserted by Ordem dos Enfermeiros (OE), and OM should assert the attributes related with the practice of physicians. Consequently a set of authoritative sources

may need to be consulted by service providers before the latter grant users access to the resources they want to access.

Other attribute authority sources should be considered for Identity Provider such as other professional classes. Table 3 represents the IdP for each professional class represented in eHealth environment. Source authorities for patients are represented by the National Registration for Patient Identifier. Other repositories are also needed such as Entities identifier, for a National Entities Identifier and healthcare professional's lifecycle and working location.

4.5.1.2 User registration and service subscription

The identification procedure is the mechanism through which the patient or healthcare professional identify themselves before an authentication token is given out, and the assurance quality level will depend on the level assigned to the identification procedure. For higher level of quality in the user identification procedure, physical presence is usually required, at least when the identification of the claimant requires a physical meeting with the claimant during the registration process. This must happen at least once and it may be not required for a renewal. In this case quality of assertion is at least refer to some unique piece of information that only the user is assumed to know, such as his/her patient identifier number, his/her social security number, and that can be checked against some official register, authorities sources of Identity, resulting in a a unique identification. The validation of the assertion can require the assertion to be signed with a non-qualified digital signature.

Portuguese Citizen Card is issued with high quality levels of the identification procedure, and the higher the quality of the issuing procedure [94], the stronger the binding between the claimants identity and his real-life identity in the successive electronic authentication phase. The highest level, limited to the issuing process, is reached when the delivery is conducted in the physical presence of the claimant. In order to obtain an highest level in the overall registration phase the delivery in person must be associated with the highest identification process; this requires that the identity of the receiver is validated using an official government identity document, either at the location of the issuing party, or by authenticated delivery at location selected address.

The citizen card has a set of attributes such as the patient number. Although the citizen card has an high quality level for identification and issuance, the management of the patient number is independent of the citizen card.

The process for patient identification and registration, responsible for the assignment of the patient number, is not sufficiently specified. Each health center sets its own identification procedures, criteria for the documents acceptance and their validity as proof for evidence for an identity and respective benefits. With the current processes for patient identification and patient registration it is not possible to guarantee uniqueness of the number, and this may not prevent that

the same number is attributed to more than one person, by mistake in the identification process. Despite the citizen card has high levels of assurance, the problem still persists for the patient number contained in the citizen card.

The IdM model will assume for the registration process, an auto-enrollment procedure. For this auto-enrollment procedure the use of an eID card is needed, for instance the use of Citizen Card. There are three different user profiles for auto-enrolment process: (a) Patients, (b) Health Professionals and (c) Entities.

For patient's auto-enrollment procedures, the actors that participate are: patients and source authorities.

The auto-enrollment process is a fully automated registration process where all evidence is made for the IdMS, allowing the patient or professional to register himself without the need to present legal paper documents. The system must be able to verify all attributes claimed by the user. Patient can opt-in to register and have access to health applications and this leads to the concept of explicit consent of the owner of the data, and the system always request patient permission before data can be sent to service provider.

The registration processes is done following a web portal access for patient services delivery, and choose the option for self-registration.

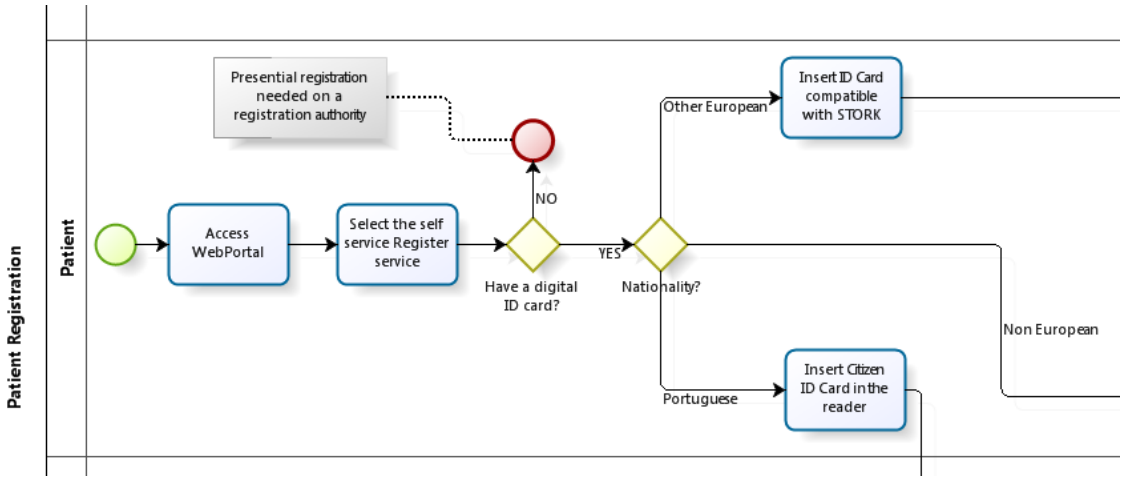

Figure 19. Patient registration process

The system will require the eID Card and depending on the nationality of eID card presented, the authority source can be National authority or European authority. For security reasons, the requirement for a valid eID card is needed to all registration process, because by requesting eID it's possible to check electronically the information given and guarantee that the person that is registering is the one it claims to be.

If the patient is not a national citizen, then the role of the STORK platform is to identify a user who is in a session with a service provider with the original country. The model is not prepared for non-european citizens and presence registration is mandatory.

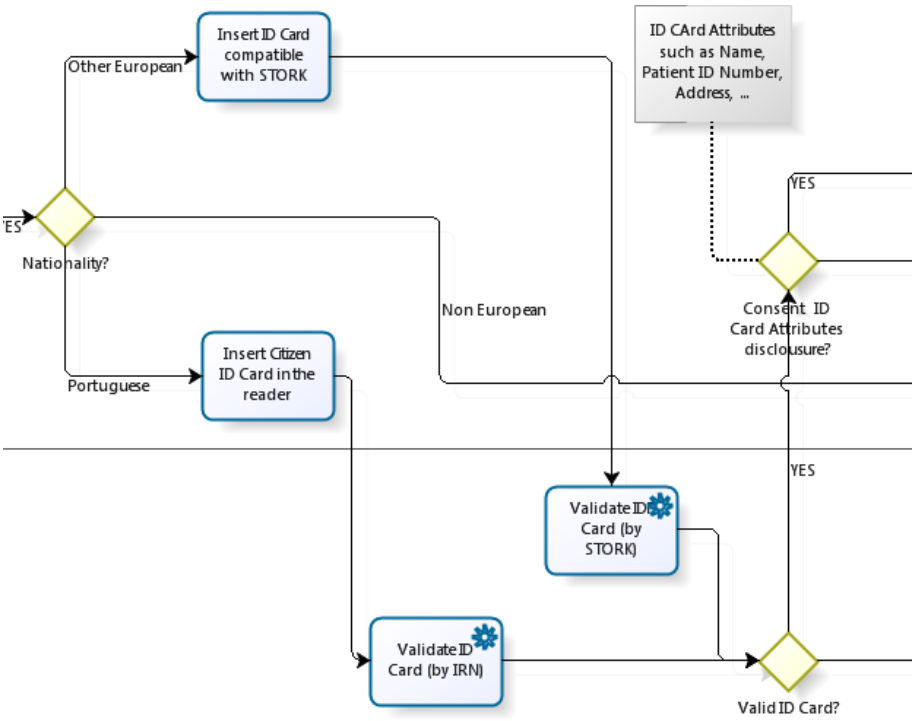

Figure 20. Citizen Identity verification and validation

If the eID is valid, and considering that the patient should be in control over personal attribute data, and minimal disclosure information should be sent and save to IdMS, the user must explicit consent. After the explicit consent, some attributes might be sent, such as patient ID, address, birth date, others.

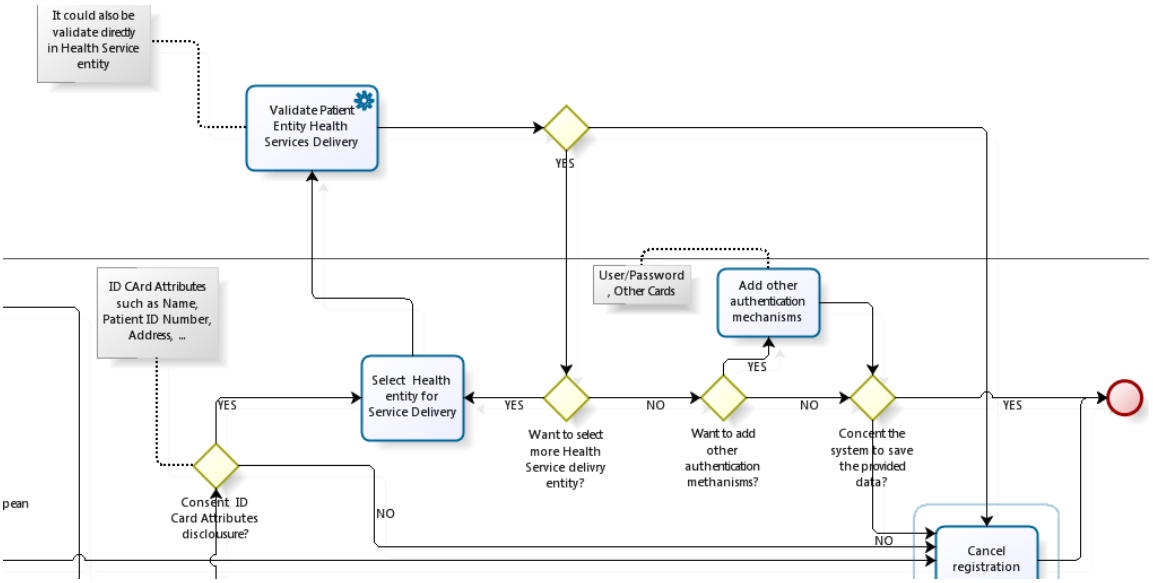

Figure 21. Associate patient registration with health entity for service delivery

The patient will choose a Health Service delivery Unit to be registered on the IdM system, and the IdM platform will verify the validity of the user attributes in the selected healthcare units, requesting the user authorization for the information to be sent for verification process. The patient can be registered in more than one healthcare unit, and validation in patient registration entity is required. Finally it is possible for the user to associate other authentication mechanism to his account. The selected mechanism will be classified with appropriate assurance level, that is discuss further on.

The user is requested to allow for saving the minimal data provided into the IdM system and the auto-enrolment is finished with success.

4.5.1.3 Anonymity and Pseudonyms use

There are no definitions of anonymity that can satisfy all cases. Many definitions deals with the simple case of not be able to relate a sender and the message, by not be able to link them or sent back a message[95] Both anonymity and pseudonymity protects the privacy of the user location and true name, where location in this eHealth context refers to the actual physical connection to the system.

The IdMS should be aware of the main issues related with privacy, however, pseudonymous are not directly related with this identity management proposal model, and is considered out of scope. Anonymity and pseudonyms should be address for example by the national patient identifier, if a patient request for anonymization. The IdMS should be able to verify the patient that claim an attribute even if the attribute is a anonymization attribute.

4.5.1.4 Privacy assurance

Privacy assurance is one of the major requirements of any IdMS, especially in eHealth since clinical attributes and the assurance for authentication and authorization entities, it is common to consider them only accessible and restrict them as possible to some entities. Attribute exchange must be defined and the IdMS should provide patients and healthcare professionals with the choice for control over the use and disclosure of their personal information.

This can be assured by controlling the attributes exchange and interoperability by the registered applications, and applications to be registered should be in compliance with privacy policies defined. Some privacy framework are being defined, such as ISO/IEC 29100: Information technology – Security techniques – *A privacy framework*, and ISO/IEC 29101: Information technology – Security techniques – *A privacy reference architecture*.

Accordingly with SAML V2.0 specifications [96], this protocol includes mechanisms that allow providers to communicate privacy policy and settings. For instance, SAML makes it possible to obtain and express a principal's consent to some operation being performed [96].

4.5.1.5 User empowerment

The importance on having a trustable and transparent system allows the user empowerment by controlling personal information requested and consent, minimizing the information stored by the system. Through logs access is possible to create features that allow the patient to obtain information on who accesses their data thereby protecting their data and also allowing fraud combating.

If the system is able to give information on accesses that have been made, and by whom, beside patient empowerment it might inhibit illicit use options from healthcare professionals on access information without the existence of a medical situation to justify it. For example, in the case of electronic prescription, if patient is allowed to access to the prescription information over the last six month of prescription, this will not only create awareness to the patient but also will inhibits the prescriber to make a bad use with electronic prescription, such as prescribing considering the patients benefits to other patients, although identify other patient with high level of benefits for cheaper medical drugs. Access to information about what was prescribed and who have prescribe will allow the patient protection and fraud combating.

Applying the Liberty best practices recommendations on privacy [97] for fair information practices are based on principles of notice, choice and control, access, security, quality, relevance, timeliness, accountability and complaint resolution.

4.5.2 Service Provider (Applications)

In the proposed IdMS the service provider is defined as any eHealth application that is registered in the IdMS. Applications can be use by healthcare professional or by patients, in different security contexts having different requirements that have to be fulfilled and interoperability by different applications. The SP requirements are described by the application contexts, application profiling, application subscription, attribute exchange and user profiles and authorization to grant privacy and secure access to health information.

4.5.2.1 Applications contexts

Health information infrastructures consist of several heterogeneous health information systems (HIS) with dissimilar data management mechanisms [98]. HIS are deployed either on a national/governmental level or on local levels such as hospitals or primary health care systems. The daily practice of healthcare professionals is mainly based on a heterogeneous local desktop set of applications, sharing the same local environment. These applications can be characterized by their high diversity and isolation, performing very specific functions without any local pre-determined system integration. From the healthcare professional point of view, this software working environment requires adaptation to many heterogeneous and different information systems. For the other non-desktop central applications, he usually spends much of his time recording data that is

mainly necessary to the control and production monitoring of the health system in health delivery. In fact healthcare professionals have to adapt to numerous information systems, desktop and server based, which are not integrated, requiring several credentials and separate identifiers that they use to identify themselves into each one of them.

4.5.2.2 Application profiling requirements

An application can be considered as a combination of processes and information resulting in some well defined outcome –accessing an individual's shared electronic health record; sending a referral notice to a specialist; sending a discharge summary from a public hospital to a GP, electronic prescription are some few application examples for eHealth. The software application security and information usually forms a key part for a risk management approach. Application classification must be done by the sensitivity data. The impact that might arise when an identity assertion is accepted as true when it is actually false should be considered in the application use. Application classification can be summarized as with following levels: (a) Level 1 Minimal Risk; (b) Level 2 Low Level Risk; (c) Level 3 Moderate Level Risk; (4) Level 4 High Level Risk.

These application classification assurance levels provide the necessary information and threshold for the minimum authentication assurance level requirements by identity authentication for users accessing the applications. Authentication level and credential types that should be used by user identity authentication should depend on the applications classification.

4.5.2.3 Application registration

The application registration on IdMS requires application identification requirements. These application requirements must be in compliance with the best practices discussed earlier. Some of the main requirements for application registration are: (i) identify the users profiles, (ii) the application authentication assurance level requirements, (iii) the application attribute identification interoperability, (iv) the URL domain and (v) the attributes needed for authentication interoperability in single sign on.

For the application a X.509 certificate is issued with extended attributes to identify the identity of the application. With the X.509 is also possible to create secure sessions either through TLS/SSL or established by identifying the application to create a trust within the managed domain by the IdMS.

The X509 certificate can also be used to digitally sign a transaction between different applications.

In next subsection some details aspects related to the exchange of attributes between applications, as well as user profiles, and application authorization mechanisms are discuss.

4.5.2.4 Application Subscription

For patients and healthcare professionals, application subscription can be done online.

After user auto-registration process, with the validity of source authorities, the user can request for a service catalog. The service catalog have all applications that are registered in IdMS, for the user profile, ie, patients are not allowed to see applications that are design only for healthcare professionals.

In figure 22 the user service subscription is presented. The user must be authenticated in a webportal, where the application is published, and then the user can request for service subscription. A service catalog should be presented and after the user selection the IdMS should validate if the user fits to the defined profiles. Then Terms and condition for service use are presented for user agreement.

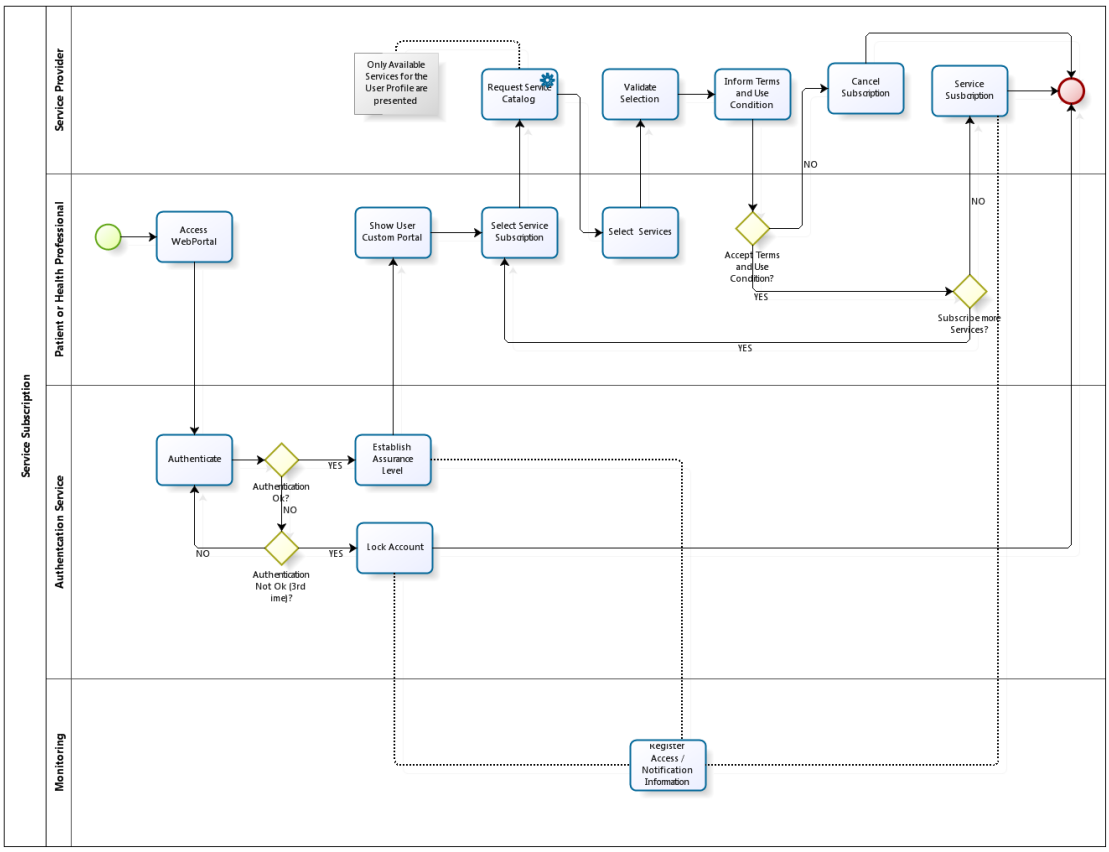

Figure 22 Service Subscription

4.5.2.5 Attributes exchange between applications

The attributes exchange promotes interoperability between applications. The IdM system and the authentication must ensure that the user has access to the resources. Authenticated identity attribute should be the initial exchange between applications to ensure that the user have

authorization to access the resource, establishing this way the initial condition for attribute exchange between applications. The level of authentication assurance is important and will be discuss further on 4.5.3.1.

In general, the sharing of patient information is required by eHealth applications. The identity system must be considered as a facilitator in the exchange process, establishing a secure communication channel for the attributes exchange and the assurance that the application identity is recognized, and the exchange can be established however the IdMS should not save attributes exchanged by the applications

After securing the communication channel the Identity management should only moderate and not take an active part in this process. For legal compliance, it must be ensured that: (i) the patient attributes exchanged, have the patient consent, authorizing that their personal information can be exchange for another context; (ii) Information to be exchanged securely, encryption mechanisms must be used between the applications, protecting the message for example form *eavesdrop;* (iii) The trust required between applications to exchange information is needed, and using digital certificates is necessary to ensure that the identity of the application can be recognized.

4.5.2.6 User profiles in applications

Applications usually have different user profiles and roles associated, and Identity authentication established an authentication session of the user with attributes verification with the assurance level on the level required. However the user profile (role) in application, for example be hospital administrator, is out of scope. User roles and functions must be recognized within applications. IdM model should use the authentication and qualification methods for user identity asserter, and roles and functions that user have in a specific application should be in the application asserter responsibility.

If the user belongs to a membership of a group, for example physician practice that can be verified with an source authority, IdM can exchange in the authenticated session, the relevant attributes associated with the qualification identity asserter, for instance specific rules based around such matters as user attributes, time of day, location, user identifier qualification as physician, specialty, and the status for practice. But if the application do not allowed that specialty or that source location, these rules should remain on the decision of the application level.

4.5.2.7 Authorization application mechanisms

The access mechanism for application authorization, are responsible to authorize the resource access. This authorization may be based on professional qualifications, which can allow access to generic applications, eg electronic prescribing. This means you can be allowed access because they have a medical qualification, to a set of applications. Another example might if the source location is from particular entity, a set of applications can be available.

Application authorization must be given to users when it comes to applications where not all qualified users have the same kind of access, for example an application that not all physicians can access, only those with the expertise of obstetricians is that they can have access.

Another example might be on electronic prescribing only certain medical specialties can prescribe certain drugs. This requires that the attribute for professional qualification in medicine and the attribute for medical specialties must be exchange to the application, leaving the business rules in the authorization for prescription to the electronic prescribing application.

4.5.3 Authentication

In the authentication phase, the proof of identity is given by the credential or token that the user present, and it authenticity is verified. The quality and assurance of this phase depends on the type of the credential or token that is used, the quality of the credential or token delivered, the authentication protocol used for the authentication check, and the mechanism used to communicate the result of the authentication to the user. We may consider two types of for individual authentication, identity and attribute. Identity authentication is the confirmation process of a person identity, and attribute authentication is the confirmation process of a person qualification, allowing qualifying the person in a particular group for example patients with diabetes, healthcare professional, etc. For attribute authentication, it is necessary to establish the level of confidence that an individual possesses a specific attribute that he is claiming to have. For example when a patient is claiming for a benefit, the attribute authentication for the benefit must be check for it validity and the level of confidence is made on the patient attribute depending on the verification process. There are several types of token that can be considered for authentication, and the most common types are [94]:

Username/Password or PIN: is a character string that the user should keep secret. This is the most used token and usually is used when for low-risk services. Often, the passwords might be generated by the system or the system may enforce for strong passwords. When the identity provider allows the user to choose a credential, it is important that the system enforce for strong password to be chosen.

Password list: can be a set of PIN codes that can be combined with a static password or PIN within the authentication system. Typically a password list may be a card with a set of PIN that the user is challenged to give under certain actions.

One-time password device: Is a hardware device that generates a "one-time" password that is valid for only one authentication session.This type of credentials are usefull for application authentication for attribute exchange since the, a challenge is sent from the verifier for authentication.

Soft certificate: digital certificate that can be stored locally on media. For authentication the digital certificate is accomplished by proving the possession and control of the key. Usually the soft certificate is encrypted under a key derived from a private password that is only known by the user and the use of the private key is required to activate the certificate.

Hard certificate: is a smartcard or similar media that contains a protected cryptographic key, for example an eID card. The user authentication is performed when he provides the possession of the eID card and the knowledge of the PIN.

4.5.3.1 Security of the authentication mechanism

The security of the authentication mechanism and the level of trust can depend on the authentication mechanism used and on its security. Threats like identity theft may happen when the authentication mechanism is compromised. Usually these kinds of attacks can be done by social engineering, where the attacker gains access the user authentication credentials usually by faking his identity. Other threats might come from attacks directed only to the authentication protocol itself and identities can be stolen via a list of attacks against the remote authentication procedure. The Identity theft attacks can be done by the via the following methods[94]:

Guessing when passwords are too simple or have some logical information associated to then, the attacker tries to guess the password. This attack works in cases where the secret is weak. Some common attacks are guessed by using dictionaries.

Eavesdropping is an attack that consists in scan the messages passing through a communication channel. The attacker launches successive attacks after analyzed the messages and generally he fake the user identity by delivering the user credential.

Hijacking is an attack that consists in taking over a user authenticated session by an attacker and to have access to sensitive information.

Replay is an attack where the messages are repeated or delayed messages and the system recognized them as valid messages. The attacker can reproduce transactions or gain access to sensitive information.

Man-in-the-middle is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all messages going between the two victims and inject new ones.

4.5.3.2 Assurance Levels

The level of security and authentication mechanisms are related to the proper degree of certainty we have about the degree of certainty that the user has presented an identifier that

represents the identity. The process needed to establish the identity identification and the registration process should be based on a risk assessment on how the information was obtain. The assurance level should increase the trust and minimize the risk associated with poor reliable information. For the proposed model, the information will be in four different level. For each level, the authentication mechanism used should be more robust and reliable. The levels for information can be classification is: (1) Controlled Unclassified Information; (2) Confidential; (3) Secret and (4) Top Secret. The information classification is important since it is possible this way to determine of the right level of assurance needed for information access, and to recognized the impact that a wrong access might have. Some of the most common criteria for assigning assurance and access level are:

Level 1 authentication is used when there are little or none requirements for confidence in assertion, and minimal assurance is guarantee. This authentication level when compromised will produced a minimal damage from the assertion being accepted as true when it is actually false. This means that the user is not the person it claims to be. The damage caused might will produced a (a) minimal inconvenience to any party, (b) no risk to any party's personal safety, (c) no release of personal data to third parties, (d) minimal financial loss to any party, (e) no damage to any party's standing or reputation, (f) no distress being caused to any party, (g) no threat to organizations systems or capacity to conduct the service, or (h) would not assist a crime or hinder its detection.

Level 2 authentication is used when there are some need for confidence in the assertion and low assurance is guarantee. When compromised the damage from the assertion being accepted as true when it is actually false is considered to be minor. In this case the damage may follow the situations for: (a) minor inconvenience to any party, (b) no risk to any party's personal safety (c) no release of personal data to third parties (d) minor financial loss to any party, (e) minor damage to any party's standing or reputation, (f) minor distress being caused to any party, (g) no threat to organizations systems or capacity to conduct the service, or (h) would not assist a crime or hinder its detection.

Level 3 authentication is used when moderate assertion is required and moderate assurance is guarantee. When compromised, the damage from the assertion being accepted as true when it is actually false is moderate. In this case the damage may follow to the following situations: (a) significant inconvenience to any party, (b) no risk to any party's personal safety, (c) the release of personal sensitive data to third parties, (d) significant financial loss to any party, (e) significant damage to any party's standing or reputation, (f) significant distress being caused to any party, (g) moderate threat to organizations systems or capacity to conduct the service, or (h) could assist a crime or hinder its detection.

Level 4 authentication is when substantial damage can be done from the assertion being accepted as true when it is actually false. Huge damage might be caused and the following situations

can be applied: (a) substantial inconvenience to any party, (b) risk to any party's personal safety, (c) the release of personal sensitive data to third parties, (d) substantial financial loss to any party, (e) substantial damage to any party's standing or reputation, (f) substantial distress being caused to any party, (g) significant threat to organizations systems or capacity to conduct the service, or (h) could assist a crime or hinder its detection.

Determining assurance levels required will conduct for the selection of the authentication solutions mechanisms that should be applied to resources access. The user should be challenge for increased the assurance level every time he needs to access information classified with higher levels.

4.5.3.3 Cryptographic Tools and Secure communication

Mainly in eHealth information are under the needs of authentication assurance levels, 3 and 4, since the information is sensitive and usual in the spere of the patient and healthcare professional that is delivering health services. To protect the release of personal sensitive data to third parties, and in the result from the assertion being accepted as true when it is actually false, it is proposed tree authentication mechanisms, for patients and health professionals:

1. Credentials with user and password –related with the assurance level needed and the proof of ownership requirements;
2. National eID Card, the Citizen Card with a digital identity assertion in national authentication framework, or foreign eID card, belonging to a European country, with a digital identity assertion in STORK authentication framework;
3. Professional ID card associated when the user register to the system;

The system will accept the some authentication mechanism for professionals and patient although professional ID cards, will only be possible for professionals and they can be associated with professional chamber or organizational policy.

All credentials must be given safely and with the aim of ensuring non-repudiation for those receiving the credential. The authentication mechanisms must be made on secure communication channels using adequate mechanisms such as TLS/SSL channel, PKI certificates, and others. The mechanisms used for authentication of a professional or patient are directly related to the degree of trust that he is who he claims to be, and with the required security level, for which the resource is classified.

Depending on the communication channel being on a private or public network, the required authentication assurance level should be increased from level three to level four respectively.

4.5.3.4 Credentials and proofs of ownership of credentials

Identity credentials are used to represent one's identity in electronic health service delivery, it is important to assess the level of confidence in the credential. The credential provider should issue and maintain the life cycle of the electronic credentials. The credential provider must assure full compliance with the authentication assurance levels.

The policy for issuance and maintenance credentials should enforce the authentication process trustworthiness. Credential assignment must be complied with the all process/technology requirements for assurance the Levels of assurance, and a user with level 3 assurance authentications may use a credential to be authenticated for a transaction requiring assurance Levels 1, 2, or 3.

4.5.3.5 Resources access

In the IdM model, resources access can be represented by the workflow defined in figure. The method used for authentication gives to the session an assurance level. If the user request access for an application, that is classified for an higher assurance level, then it will be ask to the user a new challenge to improve the assurance level to the one the application demand. If the user is already authenticated in a high level of assurance level, the session will forward the user to the requested application.

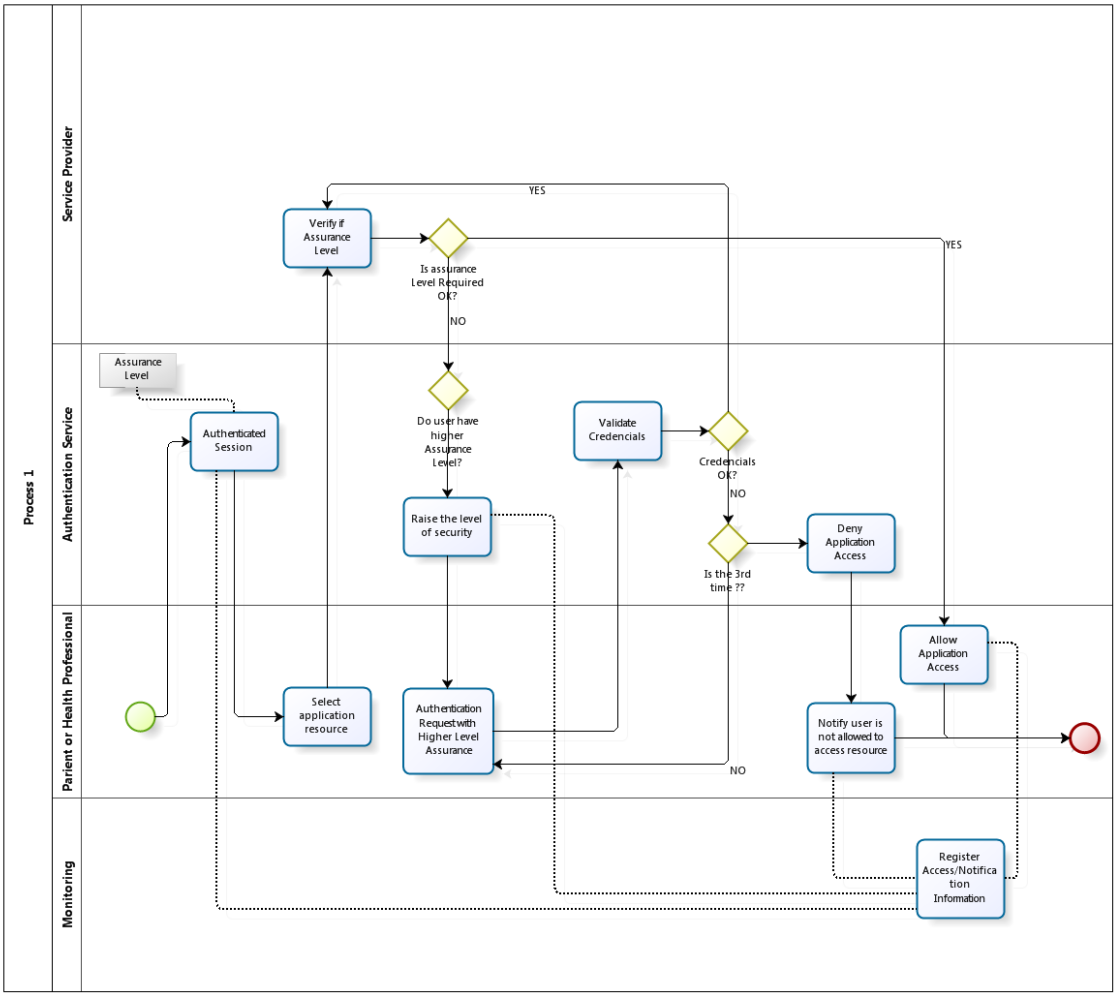

Figure 23. Process for IdM Resources Access

4.5.4 Monitoring, audit and control

There are some important activities that have to be considered in the IdMS, such as monitoring, audit and control to guarantee that proper use is being made and policies are been accomplished.

The IdMS monitoring activity must consider the following activities:

(1) Information access

- Log improper attempts to obtain unauthorized access levels;
- Log verification/validation attributes messages that don't match the information provided;
- Ensure that access levels are appropriate and in accordance with the levels defined for each application/information access;
- Ensure that information is accessed by the authorized users, and that privacy policies are met;

- Ensure attributes interoperability is established in a secure way;

(2) Access establishment and modification

- Log and show the latest access - gives evidence of possible intrusions into the system caused for example by obtaining unauthorized access to the session, credentials, or misuse and abuse accessing information;
- Applications must be prepared to provide information on modifying and/or conducted accesses. This information shouldn't be stored in the IdMS, but should be provided by consulting the application. Some examples are eprescription application registered in the IdMS that should give information to the patient about the last three prescriptions, or for Electronic Health Record, information about the last access made by the patient and by the healthcare professional.

(3) **Avaliability** is one of the tree principals of security information system, in conjunction with integrity and confidentiality. For the IdMS is fundamental the highest availability perform, since several application will be published and the system must be available for applications interoperability and applications access.

(4) Identity providers services are also important to monitor availability since for real time information, attribute verification and validation services must be available and should give information on the availability of the services.

(5) Access control

Business process for compatibility activities and access rules are defined by source authorities as already seen before. The IdMS is the technology for implement the business and legal rules and policies. Information about the performance of the system and changes to the policy rules should be approved by the identity source authorities.

Audit control

The audit and control mechanisms are essential to ensure that the system is compatible with the defined policy, and that procedures are implemented in accordance with what is defined.

There are some information system audit considerations [99] such as:

- Information systems audit controls - audit requirements and activities involving checks on operational;
- systems shall be carefully planned and agreed to minimize the risk of disruptions to the IdMS processes;
- protection of information systems audit tools - Access to information systems audit tools shall be protected to prevent any possible misuse or compromise the system security policies.

Automating process

Automating the management system process it minimizes the risk of compromise security information and assure that the management and administration actions on the system follow the policies defined.

Through IdMS, the identity source authorities should have automated process in their approach, and being able to manage real time and manage access policies for each user with what is appropriate for the user's role. The identity source authority can accept, suspend, or disable those access rights. By automating process, the IdMS is able to minimize the risk by not having professionals accessing to the system that are suspended or not recognized by their source authority. The ability to monitor the use of the system is essential to ensure that the use is compliant with the established rules. The fact that the system is flexible allowing auto-provisioning of accounts and applications, requires a higher monitoring and control in their use and by automating process will improve the system quality to be compliant with the system policy.

Security incidents

Information security has been defined as encompassing systems and procedures designed to protect the system information assets from disclosure to any person or entity not authorized to have access to that information, especially information that is considered sensitive, proprietary, confidential, or classified [100].

Monitoring security incidents and defined actions procedures to mitigate the incident and the impact it might have. These processes approach for information security management [99] evidence its users to emphasize the importance of:

- understanding an organization's information security requirements and the need to establish policy and objectives for information security;
- implementing and operating controls to manage an organization's information security risks in the context of the organization's overall business risks;
- monitoring and reviewing the performance and effectiveness of the ISMS;
- continual improvement based on objective measurement.

Several requirements are needed for managing information security incidents, such as:

- Procedures to report information security events and weaknesses detected:
- Responsibilities and procedures;
- Learning from information security incidents;
- Collection of evidence

Privacy assurance and complain process

The goal of the IdMS infrastructure is to be transparent with attributes exchange and information access. The IdMS puts the decision on attribute disclosure on the patients. To assure privacy to the patient, there should be enough information on the complaint process for the patient report/complain about privacy issues detected.

It is important that the patient and healthcare professional can be inform about their rights and about the policies on terms and conditions of use. Whenever the user feels that their privacy has been compromised, an automated process must be defined accomplished with an auditable process in order to report occurrences and treat them to ensure that policies compliance are met.

5 USE CASE SCENARIOS

In this chapter some uses case scenarios of the proposed model instantiated in the eHealth environment are described.. In particular, involving the system model, actors like patients, physicians/nurses users and assumptions.

The use case scenarios are described, with a concrete example of the practical applicability and utility in the proposed model. While the purpose of the use cases is to give a rather broad view of the scope of the eHealth identity management services defined, the use case description illustrate how the model can be applied, in day-to-day situations and improve the security and quality of the delivered health care.

Having in mind the desired outcome of this model, centralized in the reality of physical identification to digital identification - defining requirements for eHealth National Identity Management System, the selected use cases can be very different in terms of privacy requirements, security levels and the way they can exist in combination with eID or other authentication mechanism. The selected use cases should be considered as representative examples.

5.1 Use case 1: patient auto-enrolment

Ehealth services are considered to be a good complement to traditional healthcare service delivery, even among older people. However, they need to become aware of the eHealth alternatives that are offered to them and the benefits they provide [101].

It is therefore being accepted by users the use of electronic services and for this reason some services are offering the patients the advantages to get health information and to request services online simplifying the eHealth services access. However, the correct patient identification is need, and online fraud is considered a high risk whereas security is a major concern. For this reason, a robust and secure auto-enrolment process is necessary.

Use case 1 describes patient auto-enrolment process, regarding privacy requirements, security and the use eID and other mechanisms.

It is very important to distinguish between three different kinds of use-cases: a) Patient identification and registration for patient ID, b) patient online auto-enrolment (register for getting online access to the IdMS), and c) when the patient is already registered and carries out consent (eg, allowing information exchange or obtaining information or service information). The main difference is that in the latter case, the patient is already authenticated with eID, issued by government-issued identification card, and for this later case the eID might not be required after

the auto-enrolment process, depending on the IdMS and application policy being complaint with application access level required.

Therefore auto-enrolment is described as:

Actors: Patient; eID Identity provider; Patient Identity Provider; IdMS Online eHealth services

Scenario

- Patient access to the online eHealth Services webportal and select the auto-enrolment registration process;
- The patient is asked to identify himself to the IdMS, with an eID card.
- After the patient identify himself, the IdMS will check information with eID identity provider and with patient IdP;
- After information check, eHealth services can be subscribed (eg ePrescription, wait time for surgery, EHR services)
- The patient is allowed to select different authentication methods for future use, although these authentication methods have to be aligned with services requirements levels. Information should be given to the patient.
- The registration is complete and the patient, receive the credentials for other methods selected (passwords, professional ID Cards, …)

The patient navigates to the online eHealth services portal website with a SSL connection, and verifies the portal website certificate. This way patient makes sure that the browser indicates a secure session.

Then the patient connects the eID card with the PC. Secure requirements for the card reader should be given, since security can be compromised if the PC has trojan installed. In this use case, it is assumed that the process for reading eID is secure. At this moment the eID is unknown to the IdMS. Three possible types of eID are recognized by the system for auto-enrolment process and should be selected by the patient:

- **A national citizen with eID card (Cartão do Cidadão)**, for national citizen the characteristic is that this type of user is regular, frequent, and the person seeking care may be accustomed to using national health services. The national system may have some information available from previous encounters.
- **If the patient is a foreign citizen resident in Portugal**, using *Serviço Estrangeiros e Fronteiras* (SEF) Card identification should be used. The distinguishing characteristic is that this type of patient ID has valid period established by SEF, and it can be

revoke at any time for some reason. These foreign citizens may have some identification information available from previous encounters.

- **Other European eID card, recognized by STORK, for foreign citizen visiting Portugal should be used.** The distinguish characteristic is that this type of patient is visiting or in business for a short period of time, irregular, infrequent, and the person seeking care is not accustomed to use national health services.

The patient should be redirected to the authentication service portal, and should type in the PIN of the card in order to authenticate. After authentication process, session is sent back to the eHealth services portal, with an authenticated session.

The patient logs into the eHealth services portal website and the server initiates a user session. Then the patient identifies him or herself, by typing in the PIN to allow the eHealth services portal website read the respective data from the eID card, such as: patient ID, name, address, date of birth.

The server verifies the trustworthiness of the patient information; check for valid eID card certificate signed by a certification authority (CA) and be able to read information attributes required by the eHealth services website portal for the auto-enrolment process, such as patient number, name, birth date and address.

The patient follows instructions in order to complete the auto-enrolment process, and electronically approves or authorizes a data exchange for validation process of the health services delivery necessary by the eHealth services.

Online services for the available applications are presented and patient may select the application to subscribe. This can empower health organizations to develop their own eHealth application keeping the publication method standardized to the patient. From the patient perspective the eHealth services portal website gives him/her access to all available eHealth application in single sign on.

Finally the patient may select different authentication mechanisms associated with the registration account, and customized options, for example on alerts on privacy issues.

The patient completes the auto-enrolment with success, and it is sent credentials (username, passwords). The patient logs off.

The use of a national eID card would open opportunities facilitating the online registration process. For the patient the advantage is obvious: besides not having to carry different cards, the patient would not have to appear in person at any health facility in order to register with online eHealth services.

5.2 Use case 2: professional auto-enrolment

Actors: Healthcare professional; eID Identity provider; Healthcare professional source authority for qualification provider; IdMS Online eHealth services

Scenario:

- Healthcare professional access to the online eHealth Services webportal and selected for auto-enrolment registration process;
- The healthcare professional is asked to identify himself to the IdMS, with an eID card.
- After the healthcare professional has identified himself, the IdMS check the information with the eID identity provider;
- Healthcare professional is ask for the professional activity, and the given information is check with respective IdP for qualifications attributes;
- Healthcare professional has to choose the working place and this information is check with the health organization or by a backoffice;
- After information check, eHealth services can be subscribed (eg ePrescription, EHR services, others)
- The healthcare professional is allowed to select different authentication methods for future use, however these authentication methods have to be aligned with services requirements levels. This information must be given to the professional.
- The registration is complete and the professional, receive the credentials for other methods selected (passwords, professional ID Cards, …)

The healthcare professional navigates to the online eHealth services portal website with a SSL connection that verifies the portal website certificate. This way healthcare professional has the guarantee that the browser indicates a secure session.

Then healthcare professional connects his/her eID card with the PC and select the option for auto-enrolment "Healthcare Professional". The same procedure considered for the patient auto-enrolment is done and once again secure requirements for the card reader should be given, since security can be compromised if the PC has trojan installed. As in the use case 1, for this use case, it is also assumed that the process for reading eID is secure. At this moment the eID is unknown to the IdMS and the three possible types of eID recognized as citizen are applied to the professional, and for auto-enrolment process the professional should selected one of the three distinct types of the following use cases:

- **The healthcare professional is a national citizen**, for national citizen, the national system may have some information available.

- **A foreign healthcare professional resident in Portugal and registered in SEF**, for example a professional that specialized in an European Country, registered in SEF.
- **A foreign European professional resident in Portugal with a foreign eID**, the foreign country may have some information available.

The healthcare professional should be redirected to the authentication service portal, and should type in the PIN of the card in order to authenticate. After authentication process, session is sent back to the eHealth services portal, with an authenticated session. If the healthcare professional is a national citizen the authentication web portal is "Cartão de Cidadão" authentication webportal [102], for SEF the same authentication service should be provided by SEF and for European healthcare professional, the authentication portal is uses countries recognized by PEPS (Pan European Proxy Services).

The healthcare professional logs into the eHealth services portal website and the server initiates a user session. Then the healthcare identifies him or herself, by typing in the PIN to allow the eHealth services portal website to read the respective data from the eID card, such as: name, address, date of birth. The server verifies the trustworthiness of the healthcare professional information; and check for valid eID card certificate signed by a certification authority (CA). The IdMS will then check with the respective healthcare chambers, for example with *Ordem dos Médicos* for a valid registration and status for practice. This way the IdMS will authenticate all information required by the eHealth services portal website to auto-enrolment process.

After the validation process, the user is now a known citizen and qualified as a healthcare professional. The healthcare professional follows the instructions in order to proceed with the auto-enrolment process, and electronically approves or authorizes a data exchange for the validation process of the health services delivery necessary by the eHealth services, needed to choose de location for practice and prescription location. The system must automate all the process for checking the information with the hospital, healthcare center, or private clinic. If no automated process is available, the person responsible in the organization must check and validity of information.

After the validation process, the healthcare professional may select other authentication mechanisms, for example associate the account to a professional electronic card or user/password credentials. At this moment in the auto-enrolment process, the healthcare professional will have access to all the applications available for the profile he/she have, plus the applications available from the healthcare organization he/she works for.

The healthcare professional completes the auto-enrolment with success, and its credentials (username, passwords) are sent. The healthcare professional logs off.

5.3 Use case 3: source authorities empowerment

Use case 3 is based on a real event, published in a newspaper in May 2011, that *Ordem dos Médicos* complained about the real lack of control and assurance they have in the Health System when some medical specialties where assigned to foreign physicians . Using the IdMS, source authorities are empowered and policies can be defined fulfill the role of each actor in the Health System.

Actors: Health Ministery, Ordem dos Médicos, Columbian physicians

Scenario:

Diário de Noticias: por Lusa*18* Maio *2011,* "40 Médicos colombianos "estão a chegar" a Portugal [103]. Health ministry announced that 40 physicians were arriving to Portugal, to work in several places in poor conditions. Physician chambers, *Ordem dos Médicos (OM)*, said that the Colombian physicians could only perform general practice. The main problem detected by *OM*, was that these physicians were performing specialized practice, without specialized qualifications. For *OM* the Columbian Physicians should follow the same registration procedures in *OM*, if their qualifications are recognized in a Portuguese Medical University. After the registration process, all legal requirements are fulfill and the physicians can freely practice, where they want, not being *OM* responsible by the practice location.

Specialization practice is *OM* responsibility, and *OM* recognized for the Columbian physicians only the rights to practice general medice.

In this use case, the foreign physicians will gain access to the local health systems even if the OM hasn't recognized them. For the IdMS the only way these foreign physicians have access to eHealth services, should be if they already fulfill all the legal requirements and procedures followed by OM. This will give them the right profile, and access to applications available for their profile.

5.4 Risk assessment

Following the EU risk definitions given by EU regulation 2004/460 [104], risk assessment is a scientific and technologically based process consisting of four steps:

1) threat identification;
2) threat characterization;
3) exposure assessment;
4) and risk characterization

5.4.1 Risk assessment definitions

For risk assessment, the following definitions are according with EU regulation [105]:

a) "***network***" means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable TV networks, irrespective of the type of information conveyed;

(b) "***information system***" means computers and electronic communication networks, as well as electronic data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance;

(c) "***network and information security***" means the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems;

(d) "***availability***" means that data is accessible and services are operational;

(e) "***authentication***" means the confirmation of an asserted identity of entities or users;

(f) "***data integrity***" means the confirmation that data which has been sent, received, or stored are complete and unchanged;

(g) "***data confidentiality***" means the protection of communications or stored data against interception and reading by unauthorized persons;

(h) "***risk***" means a function of the probability that a vulnerability in the system affects authentication or the availability, authenticity, integrity or confidentiality of the data processed or transferred and the severity of that effect, consequential to the intentional or non-intentional use of such a vulnerability;

(i) "***risk assessment***" means a scientific and technologically based process consisting of four steps, threats identification, threat characterization, exposure assessment and risk characterization;

In an information technology context, assets are the targets to be protected in a risk assessment analysis. The assets of an organization are 'anything that has value to the organization'; the term *vulnerability* is applied to a weakness in a system which allows an attacker to violate the integrity of that system; and we define a *threat* as 'the potential cause of an incident that may result in harm to a system, organization or the patient.

For the first two use case scenarios described, a risk assessment will be made.

5.4.2 Methods

For each use case scenario described, the risk assessment will be performed considering the following aspects: (1) privacy requirements, (2) security levels, and (3) their existence in combination with eID or other authentication mechanism.

The identified targets for protection in a risk assessment analysis are: (1) personal data, the 'electronic identity', (2) personal health data and clinical data, (3) reputation, of the patient or healthcare professional – user trust, and (4) privacy, 'the right to be left alone'.

5.4.3 Vulnerability

The identification of vulnerabilities starts from what the user has for example eID card , the PC, to the way services are delivered such as protocols used for authentication, interoperability between identity providers, to the infrastructure services and to social engineering considering for instance, eID theft and the user behavior. Considering the following vulnerabilities characterized by each type:

User behavior

- eID Card flaws
- Vulnerabilities of the user's PC

IdMS - service delivery

- Weak cryptographyand authentication protocols;
- Weaknesses in authentication; protocols
- Weaknesses in service providers or with weaknesses protocols used for interoperability or unsecure applications;
- Weaknesses in identity providers that enable fraud or identity theft or with poor registration process;
- Weaknesses in the infrastructure services and manage/operacional services for example uncontrolled outsourcing

Social engineering

- User behavior or lack of awareness with the vulnerabilities exposure;
- eID Card theft;
- Hijacking gaining access to the user session;

5.4.4 Threats

The potential threats to the IdMS can be a malicious attacker or misuse of identity identification or identity qualification. Considering the threats described for risk assessment using eID for authentication *"Privacy and Security Risks when Authenticating on the Internet with European eID Cards"* [106] the following threats are will also be considered when applied to the IdMS model

- **Password guessing** – As already seen before, patients and healthcare professional usually choose basic passwords or share between each other passwords. Weak passwords and the possibility of dictionary-based attacks are threats that should be considered to the IdMS model.
- **Keylog** - keyloggers can record data locally and remotely from a remote location. It's considered as a threat since it might log PIN used by eID.
- **Man-in-the-middle attacks** – as seen previously is a attack where an active eavesdropping can be implemented between service providers and identity providers or between identity providers. Messages are relayed between them, making the system believe that they are talking directly to each other over a private connection when in fact the entire conversation exchange is being controlled by the attacker.
- **Browsers** - browser-based attacks are produced due to poor security coding of web applications or vulnerabilities in the software supporting web sites. Attackers may compromise trusted web sites to deliver malicious software to a unaware user, by adding scripts that keep the webserver appearance to be secure, however the user is redirect unsuspicious to another website causing malicious programs to be downloaded to the computer and sometimes allowing remote control of the computer by the attacker, with the possibility to capture information or identify theft. Patients and healthcare professionals are usually unaware users
- **Phishing** - is a way of attempting to acquire sensitive information such as usernames, passwords and other personal information by masquerading as a trustworthy entity in an electronic communication. This is considered as a possible threat to the IdMS and usually patients and healthcare professionals are unaware users of these kinds of threats.
- **Low-tech social engineering attacks** - the hacker's manipulates the user to do things under false pretenses in order to obtain information that the user would never give him otherwise. The user should be trained not to give out sensitive information without going through proper channels. However the proper

channels are not always clearly defined and patients or professionals are not always aware of this kind of threat.

- **Service provider access personal data** – applications hosted in service providers usually wants to keep more patients data than it really needs to.
- **Identity providers** with poor registration process definition
- **Patient profile information** – the possibility of several services providers to merge data and generate user profiles
- **Eavesdropping** the communication between applications attribute exchange
- **Reputation** of IdMS by misuse user credentials
- **Hijacking** – still a open session in use by a user
- Replay- capture messages and reproduced them into the system.

Considering a high level of these risks, three major risks can be considered:

- **Identity theft** – illegitimate use of identity;
- **Privacy Reputation** – disclosure of personal information, user profiling and misuses of data;
- **Fraud** – give wrong or forgery information and misuse information;

5.4.5 Risk Levels

The assessment of risk level is expressed using two parameters: ***probability*** (of the threat, ie, the probability that the attack will occur) and ***impact*** (which the attack would have if happened). To both parameters it is assign three levels, represented by the risk level:

Low	Medium	High
1	2	3

Risk	Probability	Impact
High	High	High
High	Medium	High
High	Low	High
Medium	High	Medium
Medium	Low	Medium
Medium	Medium	Medium
Low	High	Low
Low	Low	Low
Low	Medium	Low

The assignment of risk level per threat is part of the discussion process of the risk assessment. Additional to the risk assessment, a recommendation is made.

Risk Assessment/ Risk Threat	Risk 1 (R1)	Risk 2 (R2)	Risk 3 (R3)
	Identity theft – illegitimate use of identity;	**Privacy Reputation** – disclosure of personal information, user profiling and misuses of data;	**Fraud** – give wrong or forgery information or eID and misuse information;

	Threat	Use case	Probability	Impact	Risk Level	Recommendations
1	Password guessing	UC 1	Low	Medium	Low	(1) The IdMS force strong passwords, using best practices in password management and define password policy; (2) The IdMS have active monitoring for password guest attacks;
		UC 2	Low	Medium	Low	
2	Keylog	UC 1	Low	Medium	Low	(1) This is an external risk to the IdMS usage. Patients and professionals must be aware for keyloggers and recommendation on card readers quality should be made.
		UC 2	Low	Medium	Low	
3	Man-in-the-middle attacks	UC 1	Low	Medium	Low	(1) Since all transactions are made using SSL/TLS communication channels and token are generated for session validity.
		UC 2	Low	High	Medium	
4	Browsers	UC 1	Low	Medium	Low	(1) Browser will be out of the IdMS control, and they can represent harm to application use and data. (2) Awareness and recommendation on Browser policy should be given, and misuse utilization should be notified the IT responsible.
		UC 2	Medium	High	High	
5	Phishing	UC 1	Low	High	Medium	(1) It is considered as low probability since all

		UC 2	Low	High	Medium	services used by IdMS should have valid digital certificates and user awareness should be given to verify the portal authenticity.
6	Low-tech social engineering attacks	UC 1	Low	Low	Low	(1) This is an external risk to the IdMS usage. Patients and professionals must be aware for low-tech social engineering attacks and recommendations on usage and information request should be clearly given.
		UC 2	Medium	High	High	
7	Service provider access personal data	UC 1	High	High	High	(1) The IdMS should only transfer the minimal identification information, with the user consent. (2) The definition of policies and legislation on information and communication technologies in health should required the use of mechanisms for data encryption, in data transaction, production or archiving. (3) The responsible for the data must be clearly identified (4) The information of data access should be provided to patients and professionals.
		UC 2	Low	Low	Low	
8	Identity providers with poor registration process definition	UC 1	High	High (R3)	High	(1) High risk, since there is poor awareness in health domain on reliable identification; (2) lack of policies for registration; (3) lack of mechanism for identification control in the registration process
		UC 2	Medium	High (R3)	High	
9	Patient profile information – the possibility of	UC 1	Low	High	Medium	(1) The IdMS can control access to several applications, resident in

	several services providers to merge data and generate user profiles	UC 2	Low	Medium	Medium	several locations. This the data merge and considering that minimal information should be saved, the probability decreases
10	Eavesdropping the communication between applications attribute exchange	UC 1	Low	High	Medium	(1) Cryptographic mechanisms are use to minimize the probability of eavesdropping, all communication channel are secured with SSL/TLS.
		UC 2	Low	Low	Low	
11	Reputation of IdMS by misuse user credentials	UC 1	Low	High	Medium	(1) The robustness on the assurance level on the registration process must be high and it is only possible with eID card; (2) Robust mechanism and simple methods must be used. The flexibility on using other authentications mechanisms, such as professional cards issued by chamber authority have to be careful analyzed and integrated in the system.
		UC 2	Low	High	Medium	
12	Hijacking - open session use	UC 1	Low	Medium	Medium	(1) The IDMS system must have a session timout to prevent the theft of session, this reduce the risk of open session theft. (2) The impact is consider to be medium because the levels of authentication increase depending on the sensitivity of information, and the hijacker do not know the other authentication mechanism required to access most sensitive information.
		UC 2	Low	Medium	Medium	
13	Replay	UC 1	Low	Low	Low	(1) Transactions must have tokens that ensure the validity of the transaction. Typically the lifetime of these tokens are low enough
		UC 2	Low	Medium	Medium	

						to avoid that transactions can be replicated.

From the risk level assignment, healthcare professionals have more threats with higher risks than patients. Healthcare professionals can be more vulnerable to the identified threats since they can access more information, and have more permission on services use. The IdMS suites very well for the identified threats since it requires the patient consent for attribute disclosure witch minimizing the possible impact that an unauthorized use from a user might have.

Threats have been identified and a risk assessment with risk level assignment has been made. Some recommendations and model IdMS have been identified, however it is important to follow through a risk analysis to have information about the risk treatment and risk mitigation. This risk analysis is considered important as future work.

6 CONCLUSIONS AND FUTURE WORK

Software applications for the Portuguese health sector have traditionally been planned, deployed and used by different health organizations such as hospitals, public and private healthcare centers, without a common and agreed standard for interoperable identity provisioning and authentication mechanisms.

Issues related to identity management are not only structurally related to technology, but must also include a functional understanding of the activity of eHealth to be reflected in the functions, responsibilities and roles acted upon different systems by different profiles. It is important to ensure agreed upon interoperable standards and procedures for identity management and authentication, fully complied by different entities in different domains of authentication. The criteria and policies for the quality assurance of the registration procedures that are used to determine identity and their relevant characteristics, and subsequently the management of the full identity life cycle must also be defined and fully agreed upon by all the participants.

In application development, the concepts of identity management, privacy and security bring a new paradigm in application design, where data privacy, patient consent must be in the focus of design, far from the models where each application stores all the possible information without consultation and without any other interaction with users.

Application models where the patient should have the possibility to define what kind of personal information allows the exemption, requires a development-oriented for information security and privacy.

The development of infrastructures for identity management is structural, and allows regular access and application interoperability with procedures to ensure high level of assurance in the user's identification and registration. The identity management infrastructures should be implemented and managed by independent entities.

To ensure high levels of assurance is needed to develop robust services in each IdP. This process is complex because it requires: (1) the knowledge and awareness of the importance that the IdMS have recognized by each IdP; (2) the empowerment that is provided to each IdP, having an active role in the Health System; (3) the existence of parties with technical expertise to implement and control the IdP services. There are other barriers for the IdP development such as the funding for the services development for each of the IdP and their integration with the existing information systems, automating procedures.

In eHealth the development of multiple applications with very specific functions is not mandatory, but is often the quicker and easier way to meet specific requirements or deadlines. However it is important to note that this approach requires multiple and varied professional identifications and credentials, often leading to inefficient identification of users.

From the authors experience frequently it is believed that it is possible to develop models of identity management from specific applications. However, this research shows that identity management is structural and should be considered and developed separately from any application that might be published in the IdM scope.

Building a structural infrastructure takes time to design and implement. It requires a widespread consensus, and a very strict definition of policies that are not always clear in the Health System, with agencies that have their own jurisdiction in its decisions.

This thesis developed a model that clearly shows that identity management goes beyond technological issues. The technology already exists, allows the fulfillment of the requirements for the implementation of a secure system. The main barriers are related with the clear definition of the business concepts and the acceptance of the role that each entity has to assume in the activity of health information system.

The proposed IdMS model will allow us to ameliorate identity management and foster better interoperability for eHealth. It specifies the requirements for a significantly improved identification and more secure and reliable registration process, with appropriate security levels. This IdM model also provides the patient and healthcare professionals with the needed auto-enrolment facilities, by relying on the security provided by the government issued eID card.

Patients and healthcare professionals are also allowed to take advantage of other authentication mechanisms, simpler methods such as user/password or professional smart cards,provided that security and usability profiles kept on the IdM are satisfied. This should not require special technical expertise from the user and it should also not hinder the balance between the required security level assurances and patients general usability concerns. The proposed IdM also empowers patients with a better control over their personal attributes, with better defined patient authorization and consent mechanisms for identity attribute releases, in compliance with the legal requirements for personal data protection and privacy.

Finally, the proposed infrastructure is also in accordance with the principle of the minimum disclosure of information. This is achieved by having the more critical attributes directly held at their source of authority, thus promoting a better control of attribute releases from the patients, and at the same time empowering them with a better and more efficient control of data directly in its source of authority. This fosters for much better scalability on attribute verification and validation and helps the creation of a more transparent and scalable model.

The consensus of all stakeholders of the health system is essential, regarding the organization of the presented functions and the different roles that are conferred.

The contributions that resulted from this research were:

1) A literature review in health domain that characterized the main areas of research and the main barriers and issues of identity management in health and future perspectives. This literature review was started before the research for defining the most suitable model for identity management for eHealth, and was accepted for publishing in HEALTHINF Conference 2010 in Roma.

2) Characterization of the state of the art in technology areas and outside the health domain, evidence how identity management has been widely discussed and where its state the importance and maturity far greater than that in the health domain. This highlights the late arrival of the healthcare field for these new concepts;

3) Definition of a identity model contextualized in eHealth, with the characterization of the key components, roles and actors, as well as the most relevant processes that characterize the model. This model definition was published in proceedings of the International Conference on Security Technology – 45$^{th^o}$ IEEE International Carnahan 2011: "Leveraging identity management interoperability in eHealth".

4) The application of the identity model into two use cases with risk assessment. The identification of threats and vulnerabilities that privacy, security data are exposed and a discussion in detailed how the identity model responds to the different threats.

Finally, and as a result of the involvement through the Masters of Science study the working paper on the historical background of the two most relevant health information systems, which also marked the beginning of the identity in health, with patient number and influence the evolution that the health information system had to the present time.

For future work, it is considered the model implementation with source authority with professional qualification. This will demand the attribute identification and technical specification for services to be interoperable with IdP information systems and with IdMS. It is also important to set the level of quality for identification and registration that should be required of an IdP. Applications development recommendation to be privacy and secure oriented is also a important delivery to be made.

7 REFERENCES

1. ACSS. *National Patient Identifier*. 2007 [cited 2011 30 June]; Available from: http://www.acs.min-saude.pt/dis/2010/07/08/registo-nacional-de-utentes-rnu/.
2. ACSS. *Online eHealth Services*. 2011 [cited 2011 30 June]; Available from: http://www.portaldasaude.pt/portal/conteudos/servicos+online/.
3. ACSS. *Patient auto-enrolment* 2011 [cited 2011 30 June]; Available from: https://servicos.min-saude.pt/acesso/autoregisto/.
4. Santos, R., *SECURING A HEALTH INFORMATION SYSTEM WITH A GOVERNMENT ISSUED DIGITAL IDENTIFICATION CARD*, in *FMUP*. 2009, Porto University: Porto. p. 117.
5. Windley, P., *Digital identity*. 2005: O'Reilly Media, Inc.
6. Seigneur, J. and C. Jensen, *The role of identity in pervasive computational trust*. Privacy, Security and Trust within the Context of Pervasive Computing, 2005: p. 65-75.
7. FIDIS. *D4.5: A Survey on Citizen's trust in ID systems and authorities*. 2008 [cited 2011 19 June]; Available from: http://www.fidis.net/resources/deliverables/interoperability/d45-a-survey-on-citizens-trust-in-id-systems-and-authorities/doc/2/.
8. *The LSE Identity Project Report:*. 2005 [cited 2011 10 October]; Available from: http://is2.lse.ac.uk/idcard/.
9. *A Report on the Surveillance Society For the Information Commissioner, London*. 2006 [cited 10 October 2011]; Available from: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf.
10. *Database State - Report Commissioned by the Joseph RownTree Reform Trust LTD*. 2009 [cited 10 October 2011]; Available from: http://www.jrrt.org.uk/uploads/Database%20State%20-%20Executive%20Summary.pdf.
11. al, H.O.e., *What is eHealth (3): A systematic review of published definitions*. Journal of Medical Internet Research, 2005. **7 (1)**(e1).
12. Eysenbach, G., *What is eHealth?* Journal of Medical Internet Research, 2001. **3(2)**(e20).
13. Comission, E. *What is eHealth?* [cited 2010 12 December]; Available from: http://ec.europa.eu/information_society/activities/health/whatis_ehealth/index_en.htm.
14. ISO/IEC-CD-24760. *"Information Technology -- Security Techniques -- A Framework for Identity Management"*. [cited 2010 5 April]; Available from: http://www.iso.org/iso/catalogue_detail.htm?csnumber=51625
15. República, A.d., *Created the patient identification card from the National Health Service*, in *Decreto-Lei n.º 198/95, de 29 de Julho*. 1995, Diário da Republica.

16. INCM. *Imprensa Nacional Casa da Moeda*. 2011; Available from: http://www.incm.pt/site/home.html.
17. AMA. *Cartão Cidadão*. 2010 [cited 2010 15 July]; Available from: http://www.cartaodecidadao.pt/.
18. Savastano M, H.A., Pharow P, Blobel B., *Identity-management factors in e-health and telemedicine applications*. J Telemed Telecare, 2008. **14**(7): p. 386-8.
19. Peyton, L., Jun, Hu., Chintan, Doshi., Seguin, P., *Addressing Privacy in a Federated Identity management Network for EHealth.* , in *Eighth World Congress on the Management of eBusiness, 2007. WCMeB 2007.* . 2007. p. 12.
20. Hildebrand, C., Pharow, P., Engelbrecht, R., Blobel, B., Savastano, M., Hovsto, A., *BioHealth-the need for security and identity management standards in eHealth.*, in *Stud Health Technol Inform*. 2006. p. 327-36.
21. Wikipedia. *Pseudonymization*. [cited 2010 26 Jun 2010]; Available from: http://en.wikipedia.org/wiki/Pseudonymization.
22. Wikipedia. *Anonymisation*. [cited 2010 26 Jun 2010]; Available from: http://en.wikipedia.org/wiki/Anonymity.
23. L., L.I., *Multi-centric universal pseudonymisation for secondary use of the EHR.*, in *Stud Health Technol Inform*. 2007, Pubmed. p. 239-47.
24. Pommerening K, R.M., *Secondary use of the EHR via pseudonymisation* in *Stud Health Technol Inform*. 2004, Pubmed. p. 441-6.
25. ISO. *"Pseudonymization" – new ISO specification supports privacy protection in health informatics* 2009 [cited 2010 26 July 2010]; Available from: http://www.iso.org/iso/pressrelease.htm?refid=Ref1209.
26. Commission, E. *Art.29 Data Protection Working Party*. [cited 2010 26 Jun 2010]; Available from: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm.
27. MEYER, F.D., *Privacy protection through Pseudonymisation en eHealth*, L.R.-F. G DE MOOR, Editor. 2008, IOS Press.
28. Peyton L, J.H., Chintan Doshi, Seguin P., *Addressing Privacy in a Federated Identity management Network for EHealth.* , in *Eighth World Congress on the Management of eBusiness, 2007. WCMeB 2007.* . 2007. p. 12.
29. Mina Deng, S.R., De Cock D, Preneel B, Joosen W. , *Identity in federated electronic healthcare.* , in *Wireless Days, 2008. WD '08. 1st IFIP*. 2008. p. 1-5.
30. Au R, C.P. *Consumer-Centric and Privacy-Preserving Identity management for Distributed E-Health Systems*. in *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*. 2008.
31. Slamanig D, S.C., *Privacy Aspects of eHealth*, in *Availability, Reliability and Security. Third International Conference on 2008*. 2008. p. 1226-1233.
32. Al-Nayadi F, A.J. *An Authentication Framework for e-Health Systems.* in *Signal Processing and Information Technology, 2007 IEEE International Symposium on*. 2007.

33. Dagdee N, V.R., *Based Hybrid Access Control Methodology for Shared Electronic Health Records*, in *Information Management and Engineering, 2009. ICIME '09. International Conference on*. 2009. p. 624-628.
34. Hildebrand C, P.P., Engelbrecht R, Blobel B, Savastano M, Hovsto A., *BioHealth-the need for security and identity management standards in eHealth.*, in *Stud Health Technol Inform*. 2006. p. 327-36.
35. Quantin C, A.F., Fassa M, Riandey B, Avillach P, Cohen O., *How to manage secure direct access of European patients to their computerized medical record and personal medical record*, in *Stud Health Technol Inform*. 2007, Pubmed. p. 246-55.
36. EuropeInnova, I.a.S. *BioHealth Project*. [cited 2010 8 January]; Available from: http://www.helmholtz-muenchen.de/ibmi/biohealth/.
37. CEN/ISSS, *Current and Future Standardization issues in the eHealth domain: Achieving Interoperability*. 2005(CEN/ISSS eHealth Standardization Focus Group).
38. AllianceLiberty. *Alliance Liberty Project*. 2001 [cited 2010 8 January]; Available from: http://www.projectliberty.org/liberty/about/.
39. NETHA. *"Framework for Analysing, Planning and Implementing Identity Management within E-Health",* . 2007 16 July 2007 [cited 2010 8 January].
40. Comission, E. *ICT for Government and Public Services - A question of identity*. 2010 [cited 2010 8 November]; Available from: http://ec.europa.eu/information_society/activities/egovernment/policy/key_enablers/eid/index_en.htm.
41. CNPD, *Personal data protection*, in *Law nº 67/98 26 October 1998*. 1998: Diário da Republica.
42. CNPD, *Personal genetic information and health information* in *Law nº 12/2005 26 January 2005*. 2005.
43. OMédicos. *Ordem dos médicos*. 2010 [cited 2010 14 Julho 2010]; Available from: https://www.ordemdosmedicos.pt/.
44. OrdemEnfermeiros. *Nurse Code of Ethics*. 2010 [cited 2010 26 Jun]; Available from: http://www.ordemenfermeiros.pt/legislacao/Paginas/LegislacaodaOE.aspx.
45. OrdemMédicos. *Medical Code of Ethics*. 2010 [cited 2010 26 Jun]; Available from: https://www.ordemdosmedicos.pt/?lop=conteudo&op=efe937780e95574250dabe07151bdc23&id=cc42acc8ce334185e0193753adb6cb77.
46. Constitucional, V.R. *Constituição da República Portuguesa - Artigo 35º - Utilização da Informática*. 2005 [cited 2010 14 Julho]; Available from: http://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx.
47. Saúde, L.d.B.d. *Lei de Bases da Saúde*. 1990 [cited 2010 14 Julho]; Available from: http://www.sg.min-saude.pt/NR/rdonlyres/065B7F96-F9E1-4E18-AD3C-9E9425DF78FC/17033/34523459.pdf.

48. Penal, C. *Codigo Penal*. 2009 [cited 2010 14 July]; Artigo 192º e 193º]. Available from: http://www.verbojuridico.com/download/codigopenal2009-v1.pdf.

49. República, D.d. ***REGULAMENTO ARQUIVÍSTICO PARA OS HOSPITAIS***. 2008 [cited 2010 14 July]; Available from: http://dre.pt/pdf1sdip/2000/05/106B00/19371944.pdf.

50. Communities, O.J.o.t.E. *Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regardf to the processing of personal data and on the free movement of such data*. 1995 [cited 2010 14 July]; Available from: http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

51. COUNCIL, T.E.P.A.O.T., *On the recognition of professional qualifications*, in *Directive 2005/36/EC*. 2005: Official Journal of the European Union.

52. Council, E.P.a.o.t., *On the protection of individuals with regard to the processing of personal data and on the free movement of such data*, in *Directive 95/46/EC*, E.P.a.o.t. Council, Editor. 1995: Official Journal of the European Communities.

53. Cameron, K. *The laws of identity*. 2005 [cited 2010 13 November]; Available from: http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf.

54. Stork. *Stork - Secure Identity Across Boarders Linked*. 2010 [cited 2010 15 November]; Secure Identity Across Boarders Linked
]. Available from: https://www.eid-stork.eu/.

55. Hert, P.D., *Identity management of e-ID, privacy and security in Europe. A human rights view.* Information Security Technical Report, 2008. **13**(2): p. 71-75.

56. Camenisch, J. *Privacy and identity management for everyone*. 2005: ACM.

57. HANSEN, M., KRASEMANN, H. *Prime whitepaper*. 2005 [cited 2010 10 November 2010]; Available from: https://www.prime-project.eu/prime_products/whitepaper/.

58. *PrimeLife - Bringing sustainable privacy and identity management to future networks and services*. 2011 [cited 2011 25 July]; Available from: http://www.primelife.eu/.

59. Primelife. *Primelife results*. 2011 [cited 2011 26 August]; Available from: http://www.primelife.eu/results.

60. Excellence, N.o. *Future of Identity in the Information Society*. 2004 [cited 2010 16 July]; Available from: http://www.fidis.net/.

61. Alliance, L. *The healthcare challenge*. 2006 [cited 2010 13 November]; Available from: http://www.projectliberty.org/liberty/content/download/461/2946/file/HIMSS_Liberty_2006_handout.pdf.

62. TAS3. *TAS: Trusted Architecture for Securely Shared Services*. 2010 [cited 2010 27 November]; Available from: http://www.tas3.eu/project/tas3-vision.

63. TAS3. *WP7 Identity Management, Authentication & Authorization - Request for comments*. 2010 [cited 2010 27 November]; Available from:

http://www.tas3.eu/project/publications/download/wp7-identity-management-authentication-authorization/TAS3_D07p1_IDM-Authn-Authz_V2p1.pdf/view.

64. *OpenID*. 2011 [cited 2011 25 July]; Available from: http://openid.net/.
65. *OAUTH 2.0*. 2011 [cited 2011 25 July]; Available from: http://oauth.net/2/.
66. Hammer-Lahav, E. *IETF- RFC5849 - The OAuth 1.0 Protocol*. 2010 [cited 2011 23 Jun]; Available from: http://tools.ietf.org/html/rfc5849.
67. OASIS. *SAML V2.0 Executive Overview*. 2005 [cited 2011 30 January]; Available from: http://www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf.
68. Miyata, T., et al., *A survey on identity management protocols and standards*. IEICE TRANSACTIONS on Information and Systems, 2006. **89**(1): p. 112-123.
69. *Identity Federation Framework (ID-FF)* 2011 [cited 2011 25 July]; Available from: http://projectliberty.org/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications/?f=resource_center/specifications/liberty_alliance_id_ff_1_2_specifications.
70. OASIS. *WS-Trust 1.4*. 2009; Available from: http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/ws-trust.pdf.
71. *Web Services Trust Language (WS-Trust)*. 2005 [cited 2011 10 June]; WS-TRUST]. Available from: http://public.dhe.ibm.com/software/dw/specs/ws-trust/ws-trust.pdf.
72. OASIS. *Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of WS-Trust for Healthcare Version 1.0*. 2010 [cited 2011 10 June]; Available from: http://docs.oasis-open.org/xspa/ws-trust-v1.0/xspa-ws-trust-profile-os.pdf.
73. *Shibboleth*. 2011 [cited 2011 26 August]; Available from: http://shibboleth.internet2.edu/.
74. *AAI - Authentication and Authorization Infrastructure* 2011 [cited 2011 26 August]; Available from: http://www.switch.ch/aai/about/shibboleth/index.html.
75. Government, B. *eHealth Shibboleth - First testcase*. 2011 [cited 2011 26 August]; Available from: https://www.ehealth.fgov.be/sites/active.webehealthprd.ehealth.fgov.be/files/ge%C3%AFntegreerd-gebruikers--en-toegangsbeheer/cookbook/cookbook-shibboleth---first-test-case-final-nl.pdf.
76. Fedict. *Federal Public Service of Belgium*. 2011 [cited 2011 26 August]; Available from: http://www.fedict.belgium.be.
77. FIDIS. *D4.11: eHealth identity management in several types of welfare states in Europe*. 2008 [cited 2010 31 March]; Available from: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp4-d4.11.eHealth_identity_management_in_several_types_of_welfare_states_in_Europe.pdf.
78. Saúde, M., *Lei de Bases da Saúde*, L. Diário da República, I Série A (195), Lei n.º 48/90, de 24 de Agosto, Editor. 1990. p. 3452-9.

79. *HPRO Card - European Health Professional Card.* [cited 2011 9 April]; Available from: http://www.hprocard.eu/.
80. Saúde, D.-G.d. *Centros de Saúde e Unidades Hospitalares - Recursos e Produção do SNS - 2008*. 2008 [cited 2010 8 December]; Available from: http://www.dgs.pt/.
81. OF. *Ordem dos Farmacêuticos* 2010 [cited 2010 26 June]; Available from: http://www.ordemfarmaceuticos.pt/.
82. ERS. *Obrigatoriedade de registo das entidades prestadoras - Portaria n.o 38/2006*. 2011; Available from: http://www.ers.pt/legislacao_actualizada/regulacao-na-saude/822893.pdf/view.
83. DGS. *The General Directorate of Health* 2011 [cited 2011 1 May]; Available from: http://www.dgs.pt.
84. ASST. *The Authority for Blood and Transplantation Services.* 2011 [cited 2011 1 May]; Available from: http://www.asst.min-saude.pt/.
85. ACSS. *Central Administration of the Health System - ACSS.* 2011 [cited 2011 1 May]; Available from: http://www.acss.min-saude.pt.
86. INFARMED. *The National Authority on Drugs and Health Products - INFARMED.* 2011 [cited 2010 1 May]; Available from: http://www.infarmed.pt/.
87. INEM. *The National Institute for Medical Emergencies - INEM.* 2011 [cited 2011 1 May]; Available from: http://www.inem.pt.
88. IPS. *Portuguese Blood Institute - IPS.* 2011 [cited 2011 1 May]; Available from: http://www.ipsangue.org.
89. IDT. *National Institute of Drug Addiction - IDT.* 2011 [cited 2011 1 May]; Available from: http://www.idt.pt.
90. INSA. *National Institute of Health, Dr Ricardo Jorge - INSA.* 2011 [cited 2011 1 May]; Available from: http://www.insa.pt.
91. Coiera, E. and R. Clarke, *e-Consent: The design and implementation of consumer consent mechanisms in an electronic environment.* Journal of the American Medical Informatics Association, 2004. **11**(2): p. 129.
92. IRN. *Instituto dos Registos e Notariado.* 2011 [cited 2011 21 July]; Available from: http://www.irn.mj.pt/IRN/sections/inicio.
93. SEF. *Serviço de Estrangeiros e Fronteiras.* 2011 [cited 2011 21 July]; Available from: http://www.sef.pt/portal/v10/PT/aspx/page.aspx.
94. Hulsebosch, B.L., G; Eertink, H. *Project acronym: STORK - Quality authenticator scheme.* 2009 [cited 2011 30 January]; Available from: https://www.eid-stork.eu/dmdocuments/public/D2.3_final._1.pdf.
95. Pfitzmann, A. and M. Köhntopp. *Anonymity, unobservability, and pseudonymity—a proposal for terminology*. 2001: Springer.

96. OASIS. *Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0*. 2005 [cited 2011 23 June]; Available from: http://xml.coverpages.org/SAML-sec-consider-20-os.pdf.

97. OASIS. *Privacy and Security Best Practices*. 2003 [cited 2011 23 June]; Available from: http://projectliberty.org/liberty/content/download/374/2681/file/final_privacy_security_best_practices.pdf.

98. Ribeiro, L.a.C., J.P., Cruz-Correia, R. *Information Systems heterogeneity and interoperability inside Hospitals - A Survey*. in *HealthInf 2010*. 2010. Valencia, Spain.

99. ISO/IEC, *ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems -- Requirements*. 2005.

100. Hill, L.B. and M. Pemberton, *Information security: an overview and resource guide for information managers.* Records Management Quarterly 1995. **14**.

101. M. Jung, K.L., *Acceptance of Swedish e-health services.* Journal of Multidisciplinary Healthcare 2010. **3**(1): p. 55-63.

102. *Autenticação com Cartão de Cidadão.* 2011 [cited 2011 26 August]; Available from: https://autenticacao.cartaodecidadao.gov.pt/fa/.

103. Noticias, D. *"40 Médicos colombianos "estão a chegar" a Portugal.* 2011 [cited 2011 18 May]; Available from: http://www.dn.pt/inicio/portugal/interior.aspx?content_id=1854850&page=-1.

104. Council, E.P.a.o.t., *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency.* Official Journal L 077 , 13/03/2004 P. 0001 - 0011, 2004.

105. *Regulation (EC) No 460/2004 of the European Parliament and of the Council establishing the European Network and Information Security Agency.* OJ L 77 of 13.3.2004, 2004.

106. ENISA, *ENISA Risk Assessment Report - Privacy and Security Risks when Authenticating on the Internet with European eID Cards.* 2009.