Project Acronym:	***i2-Health***
Project Title:	**Interoperability Initiative for a European e-health Area**
Contract Number:	517476
Starting date:	February 01, 2005
Ending date:	January 31, 2007

Deliverable Number:	**D 3.1 version 1.0 pre-final**
Title of the Deliverable:	**Identification management in eHealth**
Task/WP related to Deliv.:	Task 3.1 + 3.2 / WP 3
Type:	Internal

Authors: **Ramin Tavakolian; ZI**

Partners: empirica Gesellschaft fuer Kommunikations- und Technologieforschung GmbH
European Health Telematics Association (EHTEL)
Technical University of Košice - Faculty of Economics (TUK).
Zentralinstitut für die kassenärztliche Versorgung in der Bundesrepublik Deutschland (ZI)
Work Research Centre (WRC)

Contractual Date of Delivery to the CEC:	**January 31st 2006**
Actual Date of Delivery to the CEC:	**June 15th 2005**

Project Co-ordinator

Company name :	empirica Gesellschaft für Kommunikations- und Technologieforschung mbH
Name of representative:	Simon Robinson
Address:	Oxfordstr. 2, D-53111 Bonn, Germany
Phone number:	+49 (2 28) 9 85 30-0
Fax number:	+49 (2 28) 9 85 30-12
E-mail:	*i2-health@empirica.com*
Project WEB site address:	www.i2-health.org

Part II:
Table of contents

Part III: Executive Summary

eHealth requires the reliable, unambiguous identification of persons, health care organisations and relevant ICT infrastructure components across all actor domains, regional, national and European health system borders. The mixture of multiple factors to establish trust known in conventional healthcare cannot cope with the new remote scenarios in eHealth, where all threats and obstacles known from the general digital world such as identity theft, loss or compromise and fragmented identities are present. IT-security management is capable to deal with these risks, but needs clear requirements to set up appropriate systems.

Multiple policy drivers have acknowledged the crucial importance of interoperability in identification management (IDM) to prevent the risk that eHealth stops at European borders.

Identification and authentication of actors are unquestioned as prerequisites to participate in eHealth. Unlike to the general commercial sector, eHealth is predominantly a highly regulated area, in which governmental authorities impose clear regulations to protect its obligatory participants. As a general principle it is concluded that characteristics of IDM systems follow their utilisation requirements.

As a base for further work some key definitions relevant to identification management are proposed in this deliverable, highlighting the fact is that yet no common terminology is applied on European policy or standardisation level. A consensus on common principles and descriptors of electronic identification is needed for the eHealth sector to overcome difficulties in comparing national systems. It must unfortunately be noted that neither the industrial sector nor the general eGovernment domain have yet consolidated such a foundation. Interoperability of electronic identification is constituted by a broad scope of aspects, covering abstract, legal and detailed technical questions. A four layer model (1. Political-Legal, 2. Organisational, 3. Semantic, 4. Technical) is proposed to support an effective comparative analysis and potential problem solving.

European interoperability of identification management in eHealth is a tremendously complex task, which bears no revenue by itself. Obstacles can be identified on all layers: entities covered by law mismatch, registration procedures differ, identifiers are not usable in cross border setting and technical carriers are not supported by other nations. Frequently national legislation specifically regulates the usage of an identifier system for a given domain, potentially prohibiting any extension.

Efforts to facilitate interoperability of identification management appear only promising for concrete use cases. A limitation of scope to patients (citizens), healthcare professionals, provider institutions and health insurances is proposed.

An approach recommended in this deliverable is to focus on 1. the mobile patient, whose administrative or medical data shall be accessed from another member state, 2. the mobile health care professional utilizing his electronic credentials in another member state, and 3. the cross border health message send between two health care professionals in different member states.

Part IV: Deliverable Content

1 Introduction: Objectives and background

The work presented in this paper (D3.1) relates to *WP 3 - Identification management in eHealth.*

Objectives

The objective of this deliverable is to cover two tasks of the i2Health work plan:

Task 3.1 Review of state-of-the-art: "*Fundamental interoperability issues concern those aspects without which no trustworthy, reliable communications on patient information will be possible. This concerns unambiguous identifiers for uniquely identifying persons, health care organisations and relevant ICT infrastructure components across all actor domains and local, regional, national and European health system borders. Any exchange of data or process oriented communication and cooperation amongst them requires the reliable, unambiguous identification of these elements. This task will collate, critically review and synthesise the European and international state-of-the-art against the framework provided from the preceding WPs."*

Task 3.2 Use cases: *"Two to four use cases from present European good practice will be identified and in-depth described and analysed. The structures and criteria developed earlier will be used to present this information, including lessons learned, for further discussion."*

The interoperability model references the overall interoperability model developed within WP 2 (D 2.1 European-level key interoperability framework, concepts, and issues) of the i2Health Project.

Background and methodology

E-Health requires reliable identification and authentication of its participants. Paramount are persons (patients, citizens, health care professionals) and social security institutions (care provider organisations and health insurances).

It is unquestioned that many other entities impose identification questions as well: pharmaceuticals, laboratory specimens, blood products, donor organs, genetic material. In some of these specific fields pan-European approaches have already been enforced.

With the establishment of electronic services new entities might be necessary for identification as well, such as system components, services, service providers, policies, and data objects. Since eHealth is new and just emerging, many specific entities are yet not comprehensively encircled e.g. harbourers of electronic patient records. This vagueness in contrast to the classical view on natural and legal persons, which has matured since centuries, is gives sufficient reason to limit the scope of this deliverable in this respect.

In healthcare the reliable identification of actors is crucial for all interactive processes. High volume uses cases like delegated diagnostic procedures, cooperative treatment, prescriptions, surveillance, and reimbursement need to proceed fluently without inconsistencies and tracking efforts. Errors or mix-up in identification of actors is high-volume issue imposing a significant economic burden for social security systems, while in individual setting the medical results might be dramatic.

Accidental mix-up of identities can be tolerated in some fields like small percentages of non attributable reimbursements claims, while being completely unacceptable for e.g. wrong donor organs.

The robustness of identification management in healthcare comes also under pressure by voluntary attacks, this might be sabotage or fraud. This topic periodically surfaces - basically if misuse or identity theft occurs. Whenever an untrained civilian achieved to misguide a whole community for long period with a faked profession, the standard question comes up: “how could that happen?”. Thereafter sporadically heads roll, security breaches are identified and some organisational directives are put into action to make reoccurrence of this specific event more unlikely to happen[1]. Until the next event happens.

In conventional setting the identification and authentication of actors in healthcare relies on multiple factors including a mixture of uncoordinated administrative measures, common sense and personal human interaction. In case of physicians we find authentic cabinets, employed staff, office telephone listings, displayed university diplomas in mahogany, big desks, business cards and name tags. Patients visit these physicians and open their deepest secrets to thembased upon reliance on various signs as listed above - but most important upon on establishment of individual trust to the person on the opposite side of the desk. Trust builds in a completely different setting as well: a patient visiting an emergency unit encountering someone barely recognizable in green garments, which only authentication might be: “...I’m the 2. surgeon on call”. Here the immense existence of a 10-floor, 600-bed hospital provides enough reassurance that this cannot be a disguised car factory.

Security is fundamental and indispensable for all IT-projects. Tools for such are structured security concept, risk or threat analysis and protection profile. For identification of actors in conventional health care these are only existing in rudiments. Here we have to face a big difference to e.g. the banking sector, which developed already long before IT-era tight control of all procedures including identification of institutions and persons involved.

Although health care had to cope with softer mechanisms of actor identification in the past, this cannot simply be transferred to eHealth because nearly all accompanying factors to establish trust in a personal encounter are not existing in electronic world. All threats and obstacles known from the general digital world apply to eHealth as well: identity theft[2], loss or compromise and fragmented identities from various origins. As consequence major IT-industries see ailing acceptance and trust in web-based services as main problem for business development[3]. For all scenarios in eHealth the proof of additional attributes such as profession or attachment to a healthcare institution is crucial and adds complexity. On the side of patient apart from the individual identity by itself, the insurance membership is of highest relevance.

[1] A notorious trickster and post employee in Germany succeeded repeatedly in obtaining high-ranking medical positions. In the late 90ies he held a position of senior consultant in a German hospital for 18 months, being praised from patients and civil servants.

[2] “The Scary New World of Identity Theft”; Newsweek, p-38-45, September 2005, New York

[3] Liberty Alliance, Whitepaper, Liberty ID-WSF People Service – Federated Social Identity; December 2005 https://www.projectliberty.org/resources/whitepapers/Liberty_Federated_Social_Identity.pdf

The scope of this deliverable focuses on European interoperability of identification in eHealth. This simply means that all services implemented in member states should work abroad as well.

In a first step this deliverable aims to deliver a definition base for terms used in identification management and describe prototype processes like the generation of an electronic identity. Currently we observe theoretical concepts and problem awareness just arising for digital identities in general[4], so that major impacts on the domain of eHealth can be expected. In a next step a modelling concept is introduced to structurize different layers or views of the overall problem in alignment with the interoperability model of i2Health.

One key area of discussion is the relationship to electronic citizen ID-schemes and eGovernment services. In these fields high volume implementation endeavours are on their way, fostered by governments of all European member states. The question, to which extent ID-concepts of entities in eHealth align to these schemes or where separation in domains exist, will nourish the discussion for years. It is aimed to contribute to problem awareness here deliver a methodology for comparative analysis. One prominent element of ID-management - the identifier is analysed in respect of its origin and qualities.

To bridge the gap to more practical usability of this deliverable few selected use cases of eHealth applications will be analysed in respect of their dependence on identification. Relevant to these use cases existing and foreseen pattern of identification management are then examined. Since further work on interoperability between nations in these priority use case requires support by national health authorities whose resources are sparse, a consensus on the selection of these use cases is crucial. This deliverable limits itself to explaining the relevance in respect of needs of patient and health care professional and legal drivers.

[4] The Laws of identity, Whitepaper, Kim Cameron, December 2005
http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

2 The need for interoperability of identification management

2.1 Political drivers

Formal statements regarding the identification issue in eHealth by European authorities are rare. In its outlined **eHealth action plan**[5] the issue of patient identification receives some attention:

"By end 2006, Member States, in collaboration with the European Commission, should identify a common approach to patient identifiers. This should take account of best practices and developments in areas such as the European Health Insurance Card and identity management for European citizens."

Appreciation of the overall problem seems to lack considerably behind current state of art. Apart from the rather isolated promotional statement "*Promoting the use of cards in the health care sector*", there is just an acknowledgement of the patient side of the problem: "*There are two types of cards that may be used in the health care sector: health cards and health insurance cards.*" Reference to a generic model of identification management or specific implementations such as digital certificates or the health professional card is lacking.

The political trail of the interoperability issue in eGovernment is long and well documented[6]. European authorities representing the eGovernment sector are well aware of a need to have interoperable ID-management for EU citizens. On 8 November 2005 the Commission adopted the first **IDABC (Interoperable Delivery of pan-European eGovernment Services to Administrations, Business, and Citizens)** work programme for the period 2005 to 2009[7]. In its eID horizontal measure the IDABC program aims to deliver a proposal for an effective eID interoperability solution for the introduction of different eID systems in member states. This activity will certainly deliver valuable foundations for eHealth identification as well, but needs to be closely linked to make preliminary results utilisable.

2.2 Legal drivers

A prerequisite of any recognition of proof of health professional identity (and attribute) is the legal cross-border recognition of the profession itself. This is provided by the **European Directive 2005/36/EC on recognition of professional qualifications**, which contains the mechanism of "automatic recognition", applicable for the professions doctor, dentist, nurse, veterinarian, pharmacist, and mid-wife.

[5] COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - e-Health - making healthcare better for European citizens: An action plan for a European e-Health Area; COM 2004(356)

[6] European Interoperability Framework for pan-European eGovernment Services, Version 1.0, European Commission, 2004

[7] IDABC Work Programme; Decision No 2004/387/EC

No attention is although given to the subject of electronic proofs for such qualifications. Electronic health professional cards containing digital certificates that are already existing in some member states are not mentioned. Its only mentioning of optional conventional cards occurs in reasoning (32):

"The introduction, at European level, of professional cards by professional associations or organisations could facilitate the mobility of professionals, in particular by speeding up the exchange of information between the host Member State and the Member State of origin. This professional card should make it possible to monitor the career of professionals who establish themselves in various Member States. [...]"

European Directive 1999/93/EC on a Community framework for electronic signatures gives sufficient legal anchoring for electronic signatures being accepted in cross border setting.

Article 5 states:

"Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:

(a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and

(b) are admissible as evidence in legal proceedings."

In principle this would urge authorities acting in one member state to accept electronic documents on professional credentials mentioned in the European Directive 2005/36/EC on recognition of professional qualifications, which were issued in another member state. Typically health professional cards contain a digital certificate containing the professional qualification, although currently no qualified ones are yet used.

Decision No 189-191 of 18 June 2003 (2003/752/EC) have significant impact on patient identification. The anchoring of the European Health Insurance Card (EHIC) is an entry into a European wide system for identification of insured members covered under European regulation 1408/71 and 574/72[8]. It is designed as an eye-readable card plastic card so that the carrier is by no means electronic, but it provides associated identifier systems for insurance providers and its members.

[8] Decision No 190 of 18 June 2003 concerning the technical specifications of the European health insurance card; (2003/752/EC)

3 State of art in identification management

3.1 Definitory foundation

Identification management of actors is far more than just the identification procedure. The generation and assignment of an identifier cannot be separated from its later usage, in particular when authentication is requested.

The term “Identification management” covers actually a broad range different aspects of granting, distributing, transporting and verifying an electronic identity. In the context of this document, identification management is seen as the corner stone for implementing the **trust model** where a requesting entity is asking for service to a decider entity, which will accept to grant this service to the requester if he is referenced by a Trusted Third Party (figure 1). In practical terms the requester might be a patient or health care professional, who has been given an eHealth Identification number. If he wants to access a service he will submit his ID to the service provider e.g. a hospital, who will have decide whether this is happening rightfully. To verify this, the requester needs to ask for a reference at the trusted third party, which issued the ID.

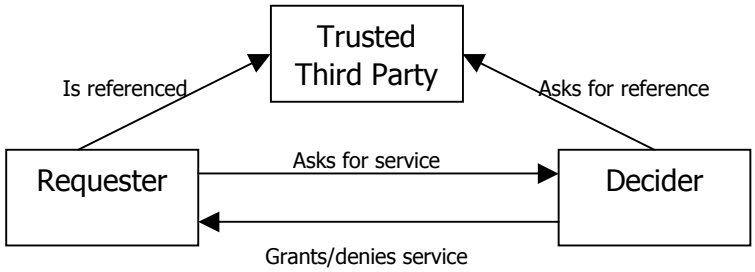

Figure 1: Trust model relationship Source: CWA 15264-1, April 2005,

3.1.1 Identity and attributes

What makes identification in eHealth specific and different from general ID-schemes is the obligatory linkage of an attribute - such as health insurance membership or professional qualification - to an individual. This linkage is normally regulated by half governmental authorities such as professional chambers or social security organizations.

With individual persons in view, we can differentiate two other constellations of linkage to an attribute. Most general is the identity delivered by the state, which is equivalent to the passport of a citizen. The state of citizenship usually claims to have the highest authority in generating and taking care of this identity. Whether this is also provided to citizens in an electronic way depends from nation to nation. This “supreme” identity will be used in eHealth applications as well, e.g. if MR Jones is identified on base of his passport to have a new donor organ implanted.

Broadly used are “deregulated” identities which follow laws of free markets: vendors, interest groups, associations or corporations may distribute electronic identities to its associated citizens, who can choose whether to participate or not. This works well in some sectors, but does not meet the requirements of eHealth, where applications are frequently obligatory

regulated by law. Comprehensive coverage of a complete population requires higher attention to data protection and privacy issues.

3.1.2 Identification

The term identification in the context of delivery of electronic health services requires at least two distinct definitions to cover its commonly accepted usage:

- assignment of a unique number (or string) to an entity within a registration procedure which unambiguously identifies the entity. This number serves thereafter as an identifier uniquely attached to this entity.

- a process of using an identifier before authorising a particular action to be performed, without verifying the accuracy of the linkage to the entity.

It must be noted that a broad variety of competing definitions are used[9]. By several sources the term “identification” is not used solely but combined with associated clarifications[10].

3.1.3 Authentication

Authentication is defined as a process to verify the claimed identity, before authorising a particular action to be performed. Alternative definitions encompass the “validation of claimed identity” and “establishment of confidence in user identity”. In principle no conflicts arise from those commonly used definitions. An aspect to acknowledge however is that more descriptive definitions include a grading or different levels of assurance; that authentication does not lead to absolute answers like “Yes or No” but deliverers assurance to the specific setting. Guidelines from the United States National Institute of Standards and Technology differentiate into four different layers of assurance of authentication. Though not formally recognized by European Institutions this model is frequently referenced and remains unchallenged.

3.2 Processes related to identification management

3.2.1 Generation of an electronic identity/granting an attribute

Ways to generate an electronic identity differ significantly for each sector. For a healthcare professional it is normally generated upon the request of the individual. Registration combines the professional attribute delivered from a competent institution with the individual identity, derived from the state, which regularly needs to be proofed by an official ID document. The attribute source might be a professional chamber or governmental authority for healthcare. The attribute source is entitled (and often obliged) to revoke the attribute. In process view the comprehensive procedure of generation and distributing an electronic identity can summarized as in Figure 2.

[9] The Electronic Identity Whitepaper of the eEurope Smart Card Initiative defines “Identification” as “Determination of the identity of a person or good”.

[10] The Authentication Policy for Interchange of Data between Administrations (IDA) released? by DG ENTR distinguishes “Identity Authentication” and “Identity Proofing” to nominate the two meanings. The Electronic Authentication Guideline (800-63; September 2004) of the National Institute of Standards and Technology (NIST) refrains from a definition of “Identification” as well.

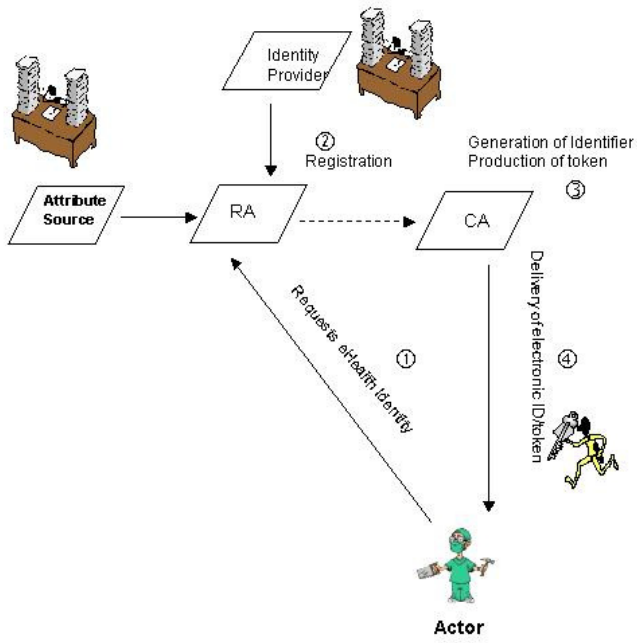

Figure 2: Generation of an electronic identity for a healthcare professional; RA - Registration Authority, CA - Certification Authority (alternatively a Credential Service Provider - CSP); the dotted line between Registration Authority and Certification Authority indicates that these entities are frequently joined into a single organisation.

Alterations of this scenario are frequently observed: the application for an electronic identity may be directed towards the attribute source, such as a professional chamber. Concentration of the involved process participants can also be observed: Attribute Source, Registration Authority and Certification Authority might be represented by the same organisation. The Certification Authority might be replaced by a Credential Service Provider (CSP) in more generic models.

A concentration of functions frequently applies to health insurance providers, which issue cards with an insured identifier. In view of patients the situation is generally more simple: from a purely medical point of view there is no need to have an additional identity apart from those delivered by the state government. Every citizen as a potential patient should have already an identifier, attached to his passport as a carrier. The security chain for these is well established, which is a result of the high volume criminal threats. In medical fields, where mismatch leads to catastrophes, such as in organ transplants; procedures explicitly rely upon these high-quality identification systems.

When it comes to reimbursement of healthcare the attachment of this citizen to a specific health insurance provider needs to be resolved. For this we encounter additional identification management systems such as for the European Health Insurance Card (EHIC). These cope with a much lower assurance level, since health insurances tend to tolerate a certain level of misuse, which could only be eliminated with inappropriate measures.

3.2.2 Entities subject to identification management

There is an extremely broad range of subjects or entities to be identified in the context of eHealth applications. All physical objects such as drugs, implants, organs, specimens and all information objects as well need to be identified. When it comes to services we find also infrastructure components like servers, repositories and tokens. In this work the scope will be limited to potential actors, which can be grouped in classical juridical sense into natural and legal (juridical) persons. This selection support the use case oriented approach.

Natural persons

Recipients of health care:

- Citizens
- Patients
- Insured members

The clear definitory separation of these groups is not trivial. Common thinking of citizens being the inclusion circle for the other two groups can collide easily; if for example an illegal immigrant receives treatment in a hospital. Some nations apply social health insurance schemes for the entire population, this can be found e.g. in Denmark, whereas in Germany only 92% of the population are covered by the social health insurances, the remaining part subscribing to private insurance companies, special schemes or having no coverage at all.

Health care professionals

- on base of a professional qualification
- on base of employment at a care provider organisation

The definition of whether someone can be considered a health professional is barely manageable in domestic setting. There are clearly defined professional groups such as physicians or midwifes, but solid proof of qualifications for many other individuals are quite difficult to obtain.

In France about 20 health professional qualifications are protected by law, while in Germany the number is likely to be around 150. We have to face a patchwork in Europe with colliding definitions for specific professional qualifications, varying levels of reassurance and inconsistent coverage by professional chambers. Several nations have integrated employees of care provider organisations into their systems, but here again approaches differ in respect of individual involvement in patient care or scope of covered institutions.

Institutions

- Health care provider institutions
- Health insurances
- Reimbursement institutions, e.g. for cross border claims clearance

Definitions vary by nature, since they reflect the long evolution of health care systems of individual member states. The view on a hospital would create little controversy on pan-European level, but fringes tend to be blurred. Attributing other institutions e.g. like

pharmacies, optometrists and patient transport company to the domain health care provider institutions might not be possible in all member states.

Out of scope remain here specific issues of overlap, inclusion, and conflict of identification management. These questions are of extremely high relevance for implementation: how to handle a single person being both physician and pharmacist? Can general ID-schemes and token be utilized to add on health professional attributes? To achieve comprehensive interoperability these problems will have to be solved, for now they would just add unmanageable complexity.

3.2.3 Authentication of an electronic identity/attribute

An actor wishing to use an eHealth service needs to provide his identification data. In all real world applications this will be accompanied by authentication data to prove that the actor is rightfully using this identity. In a step frequently required the credentials (and attributes) are verified by a trusted third party. This step is necessary, when there is a need to verify that the claimed identity belongs to the person who claimed it. This is usually done by a PIN code, but might be done in a certain future based on biometric data. The verification is also required to make sure that attributes have not been revoked. Overall, these processes are well established in national setting (Figure 3).

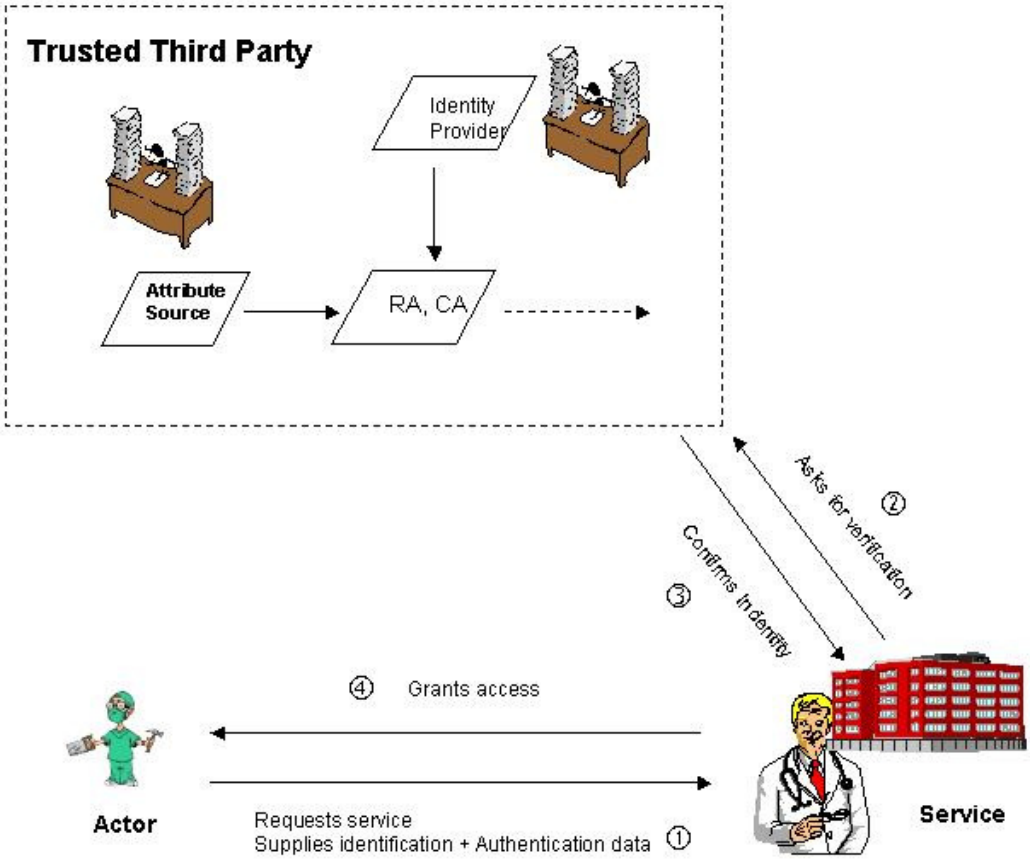

Figure 3: Verification of an electronic identity in eHealth; RA - Registration Authority, CA - Certification Authority

3.2.4 Cross border Interoperability in the trust model

In a bilateral cross border scenario this trust relationship involve two trusted third parties (TTP), if both the owner of an electronic ID (requester) and the service provider (decider) only utilize pre-existing links to their affiliated TTP. In his setting e.g. the hospital receives an electronic ID from a foreign physician and would soon notice that it is not referenced in the national verification directory from its own TTP. If a recognition agreement is existing between the two TTP, the verification request can be forwarded to the foreign TTP. Alternatively the hospital could directly verify at the foreign TTP, if e.g. a European legal superstructure nominates it to be responsible. In case of the European regulation on recognition of professional qualifications a binding European list of such reference points specific to each group will be established by 2007. In this case the hospital should find the nomination and contact details of competent authority in this list and would direct its verification request directly there.

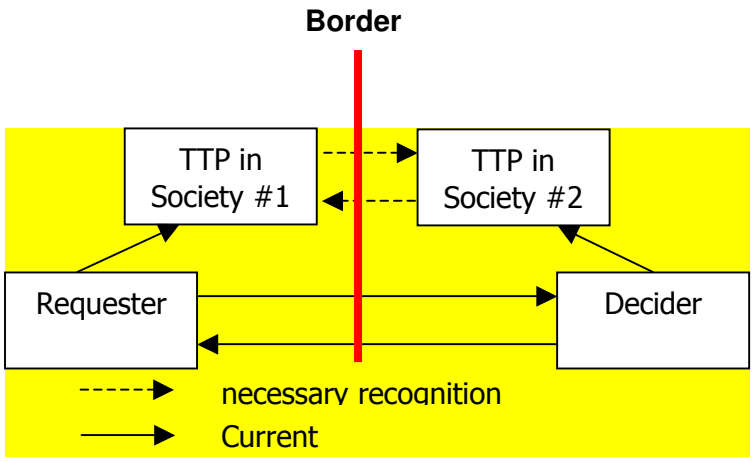

Figure 4: Trust relationship in cross border setting; modified from: CWA 15264-1, April 2005,

3.3 Conceptual model

3.3.1 Layer model

Efforts to tackle interoperability issues in electronic identification are confronted with a broad scope of aspects, covering abstract and detailed technical questions. In accordance to the overall interoperability model consented within WP2 of i2Health (figure 5) an identification management system can be described by four layers:

1. Political/Legal
2. Organisational
3. Semantic
4. Technical

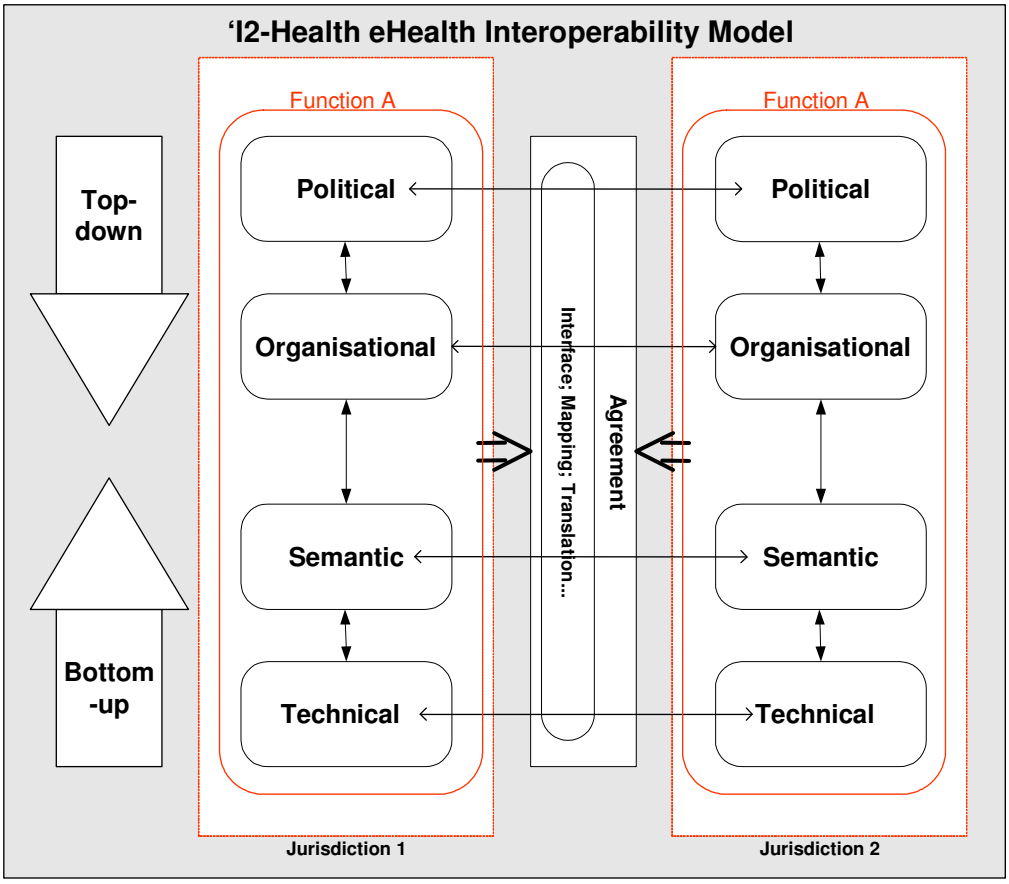

Figure 5: i2Health interoperability model

The layer model allows structuring the approach towards interoperability and helps to identify which experts/actions (technical, legal) are to involve. Applied to the specific field of ID-management the following aspects can be attributed to each layer.

Layer	Coverage
Political/Legal	Definition of scope and covered entities Agreement on trust model Nomination of competent authorities
Organisational	Registration procedures Revocation procedures
Semantic	Data model Identifier definition
Technical	ID-tokens (e.g. smart cards) Certificates Verification services

3.3.2 Application of the layer model to an example case - Dr. Dupont and his electronic physicians-ID

On **political level** national law defines that physicians are entitled or required to obtain an electronic identification as physician. Typically the usage of an electronic physicians ID is made obligatory for certain applications such as reimbursement by social security systems, participating in accredited medical training, or access to patient records. National law nominates a specific institution such as the chamber of physicians to be responsible for the generation, distribution and control of the electronic ID. In this context it is normally clarified, which other authorities are to contribute by issuing or certifying professional diplomas.

On **organisational level** the national or regional chamber of physicians regulates how the registration of a physician is exercised. This covers the definition of procedures for requesting such an ID, the verification steps performed by the chamber such as asking governmental authorities, e.g. if there are any open crime charges, and establishment of ways to revoke an attribute. There is usually some overlap between the political and organisational levels, due to a varying degree of delegative or regulatory content of the relevant legislation.

On **semantic level** the qualities of the identifier needs to be defined by lawgivers and the professional chamber. Specific requirements for data protection, privacy and implementation ease are enforced, to make sure that the identifier issued to Dr. Dupont does not collide with his citizen's and professional's rights. It this specific example the national chamber of physicians is issuing to him a random ID-number without additional semantic content to be used only for a limited period. The application of such an ID-System by the chamber is based

on preferred avoidance of longitudinal data collection on Dr. Dupont of data e.g. relevant to his prescribing behaviour.

On **technical level** Dr. Dupont receives a health professional smart card containing a digital certificate with his professional ID. The card and the certificates can be verified using a verification or revocation list database. This service is implemented by the chamber of physicians and can be reached via internet.

3.4 Characterisation of identifiers

Within the conceptual model identifiers are considered to be part of the semantic level. Embedded into identification management the semantic value or connection of an identifier is crucial for its usage. Per definition an identifier is a unique number or string uniquely attributed to an individual entity.

An identifier can be comprehensively characterized by its domain, qualities, and format.

3.4.1 Domain

Generally an identifier is only used in one domain; that implies that a specific identification number used for car spare parts might be equal to an insurance number of a patient. Problems do not occur, because all applications know well which domain they are dealing in. Interconnection of identifier systems bridging domains requires equalities of the registration procedures. The definition of which entities belong to a specific domain should be identical. Even if two nations use for example a universal system of global identifiers[11] for ambulance cars services, it might result in a mismatch, because one nation assigns a domain code for the medical sector, while another chooses a different one relevant for transport services.

3.4.2 Qualities

Closely linked to the specific domain it is used in, an identifier has characteristics describing its logical and legal embedding. These characteristics go beyond the traditional view of semantic content. An insured identifier might have characteristics, that make it very useful but dangerous from privacy point of view. Discussions between stakeholders are lengthy to find a specific solution tailored to national needs. A wide range of solutions is encountered: legal restrictions to utilize or transmit identifiers, pseudonymization services and temporary identifiers. Before fostering the usage of eHealth identifiers in cross border scenarios, it is necessary to acknowledge that these are not just simple numbers, but bear much additional complexity behind.

[11] In Germany the German Institute for Medical Documentation and and Information (DIMDI) ist adminstrating the object identifiers. OID 1.2.276.0.76, means that the object is within ISO (1), member (2), Germany (276), DIN-CERTCO (0), health sector (76)

In principle the main qualities of identifies can be described by three axes.

Axis 1 - Restriction

This quality specifies whether the identifier is designed only for internal utilization or can be open to public[12]. An example for a public identifier can be found in the USA. The Centres for Medicare & Medicaid Services (CMS) is a federal agency within the U.S. Department of Health and Human Services, which administers the Medicare and Medicaid programs - two health programs that cover about 75 million Americans. CMS contracts with private insurance companies to process Medicare enrolment applications and claims and make payments to physicians/practitioners and other healthcare suppliers on behalf of the Medicare program. For individual physicians participating in the CMS a unique physician identification number (UPIN) is required. This 6-digit alpha-numeric number is assigned upon request and displayed in public directories as long as the physician participates in the CMS scheme.

For billing purposes by CMS however a temporary billing number has been introduced to reduce risks in case of of discrimination. This number is only known to the physician and the CMS and can be reassigned upon request.

The German chamber of physicians has introduced in 2003 a system with a unique physicians ID number “Bundeseinheitliche Arztnummer” (BAN), which is assigned upon entry into a chamber. The BAN is an 8-digit alpha-numeric number, which is strictly internal to the professional chambers. Background to introduce such a restrictive ID scheme were data protection requirements in combination with an obligatory membership of the physicians.

Axis 2 - Persistency

The persistency of an identifier describes, whether it is attached for the lifespan to the entity or frequently changed. The persistency of an identifier is strongly linked with risks of identity theft and privacy violation. A persistent identifier is attached to an entity for its whole lifespan. The most permanent identifiers are biometric ones. Every individual has characteristic retinal vascular pattern, which can be used to uniquely identify this human. The danger lies however in a potential identity theft; if for example a high resolution retinal angiogram gets stolen from an ophthalmologists office, criminals might be able to fake an object, which gets accepted by scanner devices. Bad as this might already be, even the defence options if detected are restricted, because you simply cannot reassign a new retina to its innocent real owner[13]. In the administrative world there are identifiers which are almost permanent such as social security numbers, assigned at birth. These bear a risk of identity theft as well, but more relevant are questioned for opening options to make longitudinal data collection e.g. on individual consumer behaviour.

Axis 3 - Semantic load

An identifier might hold additional semantic information. The Danish social security number is constituted from the date of birth with an additional digit indicating whether the individual is

[12] The Laws of identity - Microsoft Whitepaper differentiates “omni-directional” and “unidirectional” identifiers”, less emphasizing the element of pre-designed restriction as discussed above, but the process of transmitting the identifier (broadcast or securely directed).

[13] Details of biometric identifiers can get quite confusing, due to increasing spread of organ transplant techniques. DNA-scans performed on white blood cells will reveal a mismatch once this person has undergone a bone marrow transplant for leukaemia, because the whole original white blood cell population has been wiped out by radiation and replaced by donor cells of someone else.

male or female through an even or odd number. Implications of such of semantic load are frequent: privacy aspects might prevent its utilization in setting, when the individual does not want to disclose his age or sex. In general, semantic load causes difficulties once the content information does change: just imagine the case of a sex transformation, urging the reassignment of another identifier.

The German physicians ID bears some semantic content as well: in its first two digits the region of first exercise of medical practice is coded. From this it can be directly deducted that an individual physician started his career e.g. in an east German region.

Although is has been long acknowledged in computer science, especially in data base design, that semantic load should be avoided, this has not yet fully penetrated into all sectors. Especially in social security systems identifier are used since decades or even centuries. This fact might be well accepted, but should at least be appreciated when trying to interconnect different national systems or extend the usage of old identifiers to eHealth.

3.4.3 Format

At first glance an identifier is characterized by is appearance or format. Typically we encounter definitions like “8-digit integer” or “40 digit alpha-numeric”. The format is the most simple aspect to look at, which does not provide too much difficulties in interconnecting systems. In the real world however difficulties can surface once specific character sets are involved. These are normally well established in national setting, but if it comes to utilisation abroad, other human operators and IT-Systems have to cope.

4 Use Cases for interoperability

4.1 Mobile patient

The most commonly to be expected interoperability scenario is the mobile patient. Mobility of European citizens is one of the most fundamental principles of the European Union from beginning on. Especially the aging population associated with immense increase of chronic disease imposes strain to guarantee mobility of patients. The scenario of a European citizen who becomes ill in another country and needs medical treatment can be observed in two alterations:

1. The individual needs to be identified as an insured member belonging to a social security provider of the member state of origin.
2. The insured does have an electronic patient record in his home member state, holding relevant information about his medical conditions.

4.1.1 Administrative Patient ID

The individual needs to be identified as an insured member belonging to a social security provider of the member state of origin. This identification shall support electronic transactions relevant financial flow or administrative information.

The process steps to enable his scenario are:

1. Capture of the individual ID,
2. Resolving the location of the responsible insurance provider,
3. Matching a specific request to the insured ID (e.g. verification of entitlement),
4. Transmitting the request to the insurance provider.

This use case is concrete. The electronic verification procedure of the entitlements rights based on a European Health Insurance Card (EHIC) will be performed in foreseeable future. Other use cases associated to cross border reimbursement are designed as well. The eye-readable EHIC is a carrier for an well established system with unique provider-ID and insured ID. Basically this system has its origin to the early 70ies when regulation 1408/71 regulated the procedure associated with the paper form E-111.

Application of the layer model to this scenario:

Political layer

The scope and covered entities are clearly defined by European legislation in regulations 1408/71, 571/72, and 833/2004. All individuals covered under social security systems in the European Union and associated nations are included. The use case is outlined by an immense amount of detailed regulations. It defines a broad range of general aspects like access to healthcare under benefits in kinds to specific administrative procedures such as which forms are to be send on what occasions after how many days to the responsible health insurance for notification. The individual insured is not really involved in the process. Need to give informed consent and specific data protection issues don't arise, because the scenario is comprehensively covered by legislation.

Organizational layer

The registration procedures are regulated under the social laws of the member states, since the EHIC covers exclusively aspects within this domain. We might note very significant differences in the registration procedures, which could be security weakness, overlap to other ID-schemes, such as electronic ID citizen cards, controversial identifiers that might hold discriminating information. But since these system have been legally implemented by the member states for this specific use case, no objections can arise.

Semantic layer

On semantic layer we encounter a rather simple ID system of a 20-digit insured identifier, 9-digit insurance identifier, and 2-digit nation code. By combination of these components this identifier should be unique. This appears for the use case of reimbursement sufficiently the case. The diversity of European institutions assigning these identifiers to their insured might bring difficulties to the surface: it is by no means guaranteed that a specific identifier is not attributed subsequently to different individuals; someone might have left an insurance provider and someone else gets this vacant number assigned several years later.

Technical level

The eye readable EHIC provides a carrier for the identifier. it hold all necessary information to make the use case work[14]. In its foreseen electronification this logical system give the building block to migrate into an equivalent electronic scenario.

Interoperability in this scenario

This scenario requires interoperability, since it only exists in cross border setting. Interoperability will be enforced in due time by the Administrative Commission on Mobility of Migrant Workers. Due to its very limited comprehensively defined scope, reduced of data protection difficulties, and absence of end user consent procedure however implications on other future use cases are limited.

Trust in the ID is here not a critical issue, because the system has been designed to meet the expectation of the supporting health insurance organizations in respect of mismatch. Adaptations are slow because of the obligatory firm legal anchoring process. The technical implementation of this eHealth scenario for verification of the EHIC has been proposed by the Netc@rds project.

[14] Decision No 190 of 18 June 2003 concerning the technical specifications of the European Health Insurance Card; (2003/752/EC)

4.1.2 Medical patient ID

A patient insured has an electronic patient record in his home member state, holding relevant information about his medical conditions. This medical information shall be remotely accessed to serve as a base for medical decisions in the member state of stay.

The process steps to enable this scenario are:

1. Capture of the individual ID,
2. Resolving the location of the harbourer of the medical information,
3. Authorizing access,
4. Matching a specific request to the patient ID (e.g. browse recent X-ray results),
5. Transmitting the request to the electronic health record.

The capture of the identification of an individual can be exercised by various means official governmental ID-documents like passport, ID-card or drivers license. Patients might present specific IDs usable for one specific industrial provider. Although most member states try to promote national health record schemes, these are mostly in definition phase.

The EHIC will be questionable for this function since it is not foreseen to facilitate access in domestic setting.

Application of the layer model to this scenario:

Political layer

This use case is not regulated. Different to the administrative scenarios medical information tends to be less binding but more complex. National approaches might differ insofar that the harboring institution might be the insurance provider but could as well be a separate organization. The range includes: physician organizations, national health network providers, industrials, governmental institutions, and patients organizations. The approach of a health professional towards the complex information on a patient is frequently described by the term “free assessment of evidence”. There are no fixed standards on minimum requirements for attributability and accuracy. European legal mandate bases mostly on general principles and specific decisions of the European court of Justice.

Organizational layer

It is well possible that the harbourers of electronic patient records (EPR) will have to establish own identification schemes for the patients attached, since insurance numbers might change with a change of the provider, while the EPR-ID should not. It is also well possible that the “supreme identity” guaranteed by the state is extended to such EPR access in some member states, while national privacy regulation might prohibit this in others.

Semantic layer

The identifiers utilized represent the diversity of the European Union and patient information systems in regional or sectoral setting.

Technical level

The technical aspects vary to the same degree.

Interoperability in this scenario

This scenario requires interoperability currently only for a relatively little amount of cases. Robustness is increased by the diversity of technical solutions and forces of the free market. If a specific provider wants to offer its electronic patient record or tele-consultation services also to individuals travelling abroad he should make the appropriate choices. Trust in the ID will be varying, because the derived information will be assessed on an individual base. Web-based applications are enabled normally under identification and access control features, which do not consider geographical borders. These applications will be interoperable in cross border setting simply because they do not respect borders by nature. The patient is in charge to enable access and locate the resources. More difficult is the scenario were a electronic identification is specific either from regulatory point of view or relevant to technical features such as a patient data card. The European regulation on data protection 95/46 EC provides a framework for this scenario.

4.2 Mobile health care professional

A healthcare professional is permitted to exercise his work in other member states. To enable him working in an electronic setting his electronic identification needs to be recognized abroad as well. If he is equipped with an electronic certificate on an e.g. health professional card issued in one member state, this token shall be utilisable abroad as well. From legal view he acts under the jurisdiction of another member state in this scenario, utilizing his credentials from the member state of origin.

The process steps to enable this scenario are:

1. Capture of the individual ID,
2. Resolving the location of the issuer of the professional certificate,
3. Obtaining verification for the professional attribute,
4. Authorizing access to a service on base of the professional role.

Application of the layer model to this scenario:

Political layer

A prerequisite of any recognition of proof of health professional identity (and attribute) is the fundamental legal recognition of the profession itself. European directive 2005/36/EC on recognition of professional qualifications provides a detailed framework for some professional groups.

As regards to recognition for professional purposes, it is important to distinguish between professions that are regulated from the standpoint of qualifications and non-regulated professions. If the profession is not regulated, it is subject to the rules of the labour market and the behaviour of that market and not to any legal constraints with regard to a diploma. In that case, the directive referred to above is not applicable.

A profession is regulated, when it is a statutory requirement to hold a diploma or other occupational qualification in order to pursue the profession in question. In that case, the lack of the necessary national diploma constitutes a legal obstacle to access to the profession.

The European directive 2005/36/EC applies a mechanism of "automatic recognition" for the professions doctor, dentist, nurse, veterinarian, pharmacist, and mid-wife. The directive provides a legal base for the automatic recognition of diplomas, certificates and other qualifications specified by each Member State in the annex the criteria to fulfil the minimum training conditions.

Following its entry into force on 20th of October 2005 the specific provisions (article 56) oblige the member states to inform the European Commission and the member states about their nomination of competent authorities within 2 years. By October 2007 consequently, there will be competent authorities certifying qualification attributes mentioned in the directive for cross border requests.

Organizational layer

The European directive 2005/36/EC acts on organizational layer as well. In consequence a robust legal base for equivalence of the registration procedure to obtain a specific professional attribute is set by the directive. Moreover, even the semantic aspect of the attribute descriptor is covered as well: in its annex a specific listing of all equivalent translations for the professions names affected is included. From these list it can be reliably concluded that the official German term “Hals-Nasen-Ohrenheilkunde” equals the official French term “Oto-rhino-laryngologie” and the official United Kingdom term “Otolaryngology”. This interesting example displays that although the nose is not covered at all in the English term the professional qualification is still formally equivalent.

Semantic layer

Apart from the semantic aspects of the attribute descriptor mentioned above the electronic ID of a health professional is still regulated internally within each member state. Big differences can be observed between professional groups within one member state; physicians and pharmacists might apply completely different ID-schemes, which might have regional alterations as well. With just recent initiatives to create comprehensive national health professional registers, some alignment will happen, so that cross border arrangement become realistic.

Technical level

Health professional cards are fostered in most member states as a carrier for the professional’s ID and attribute. They base in all cases on public key infrastructures, holding certificates with relevant information for authentication. The card have to be accessed using the technical infrastructure in the nation of stay, which would require interoperability of several technical elements (at least card readers and certificates).

Interoperability in this scenario

To make this scenario work high demands for interoperability especially on the technical level must be met. Once the technical difficulties in access to the ID of the health professional have been sorted out, the foreseeable extension of the European directive 2005/36/EC should provide sufficient trust for selected professional groups. The individual ID must meet some minimum requirements such as to be compliant with the “supreme ID”. In view of the relatively small amount of health care professionals involved pragmatic approaches might simply resist to support this altogether and e.g. issue another set of credentials in the member state of stay instead.

4.3 Cross border health message

An electronic message containing personal health care related information shall be transmitted between health care professionals working in different member states. This scenario is frequently encountered in the setting of tele-consultation or collaborate treatment within national setting. One physician might want an assessment or advice from a colleague relevant to specific finding e.g. an x-ray examination.

The process steps to enable this scenario are:

1. Localizing the recipient,
2. Verifying the professional attribute of receiver,
3. Composing a message with medical patient data (optional matched to specific patient ID),
4. Sending the message to recipient,
5. Recipient verifies ID and professional attribute of the sender.

Application of the layer model to this scenario:

Political layer

This use case is not regulated in cross border setting. The health care professionals act under their individual motives. Frequently recommendation or codes of conduct exist in member states for internal transmissions. Informed consent of the patient is a prerequisite to enable this scenario. The European data protection directive 95/46 EC provides a framework for this scenario if medical data are not anonymized.

Organizational layer

This scenario is equivalent to scenario 4.2 since the professional ID and attribute need to be verified.

Semantic layer

No difference to scenario 4.2 exists.

Technical level

Health professional cards are not physically involved in this remote scenario. The cards will be accessed using the technical infrastructure in the nation of issuance. More involved are elements of localization and verification, which operate in a remote setting.

Interoperability in this scenario

To make this scenario work, technical questions detached from the physical carrier of the professional ID systems surface. Aspects like trustfully resolving the location of a recipient are crucial. This mainly affects elements of the support infrastructure of applications such as trusted directories with e-mail addresses and public keys of health professionals. Apart from this the use case relies on the infrastructure for verifying professional ID and attributes. Relevant to these the same implications as to scenario 4.2 apply.

Selected literature

Electronic Authentication Guideline; NIST Special publication 800-63, 2004

National Institute of Standards and Technology

http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf

Liberty ID-WSF People Service – Federated Social Identity; Whitepaper 2005
Liberty Alliance
https://www.projectliberty.org/resources/whitepapers/Liberty_Federated_Social_Identity.pdf

The Laws of identity, Whitepaper; 2005
Microsoft, Kim Cameron
http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

European Interoperability Framework for pan-European eGovernment Services, Version 1.0, 2004

European Commission, 2004

IDABC Work Programme

Decision No 2004/387/EC