Design issues of a pan European Smart Cross Border "dream like" e-Gov Primary Health Care Medical Service

Alexander B. Sideridis [(1)], Elias Pimenidis[(2)], Loucas Protopappas[(3)],
Constantine Yialouris[(1)], Angelos Vasileios Maragkopoulos[(4)] and Andrew Chatziandreou[(5)]
[(1)] [as, yialouris]@aua.gr
[(2)]e.pimenidis@uwe.ac.uk
[(3,5)][loucas.protopappas, xatziandreoy]@gmail.com
[(4)]maragkopoulos@hotmail.com

Abstract

The European Commission of the European Union has provided Member States with the appropriate regulation and systems for the development of services facilitating cross border transactions. So far there has been little progress in putting such services to full practice. This may be justified where such systems involve the processing of confidential and personal data. Nevertheless, the proposed by the European Commission systems guarantee (as far as recent developments in network and cloud securities can do it) efficient validation of data, through authentication procedures. Cross border systems are essential in supporting one of the key principles of the EU that of free movement. Recent research and the relevant literature has witnessed the proposal and development of a few cross border systems focusing on health, social services, the environment, and life sciences. In this paper, design issues of such a cross border authentication service, linking public or/and private primary health units,are presented. The system in support of this service will offer a standard conceptual design model to interested European Member States. To evaluate the potential of such a system and its practical appeal, Greece's and the UK's primary health care services are examined. They are used as a case study of a conceptual design model applied in building up a pan European smart cross border primary health service to the benefit of citizens of any European countries being on mobility.

Keywords: e-Government systems, Primary Health Care Service, Authentication, Electronic Identification, Cloud Computing

1 Introduction

Recent literature discusses the need to design and implement e-government systems offering online services to citizens irrespective of their mobility to various countries. Most of these systems are mainly autonomous and simply connect to each other over the internet without full consideration of data privacy issues. Models used are usually of mixed structure involving automated and manual procedures [41-45].

The development of such systems has led to organizational problems and has inspired the transformation of work and service environments to digital ones [35]. In recent years systems and services, prompted by legislation and users' concerns have seen a considerable focus on security and privacy of personal data [22, 25, 33, 36-38].

Despite the switch of focus, public and private organizations in some European countries, those of southern Europe in particular, are still trying to catch up and join in the race in reshaping their organization modules [54]. Many smart initiatives, aiming to alleviate the burden of bureaucracy and to offer essential citizen services have been

launched. Almost every single one leads to stakeholders facing challenges of data integrity, privacy and security. [1, 44, 57-58].
Mobile e-Government services are continually replacing more traditional G2C services that have been designed at the start of the 21st century [40, 65]. Free citizen mobility has led to the spread of services across different systems boundaries and has exacerbated the security and privacy challenges such systems have experienced within their own country's boundaries.
Is this G2C service secure enough with regard to data integrity? Is any danger behind this service of violating my personal data? These questions are immense when private Business to Citizens (B2C) or Business to Government (B2G) are involved or when services required necessitate the use of personal and confidential data.
Various initiatives by the EU encouraging mobility of Europeans (e.g. Erasmus programmes) quite often come across bureaucracy barriers. Authenticated documents are required in support of cases bound to happen when Europeans are freely moving for studies or work, and looking for new opportunities, in general. Over the past few years the demand for services in the EU has been further aggravated by the influx of refugees that often require a disproportionate share of such services [44]. When considering the latter lack of proper identification and insecure data can cause a major problem with their mobility and integration to public life in the country there are settled.

Although online services and e-government systems have been implemented in response to mostly operational, commercial and banking requirements, the case of personal health and need for mobilization have been initially ignored. Medical files, recent additional diagnoses, certain medical examination reports, and tests may be shared, safely certified, and authenticated digitally. Such strictly confidential information is of great importance if and when is available to the appropriate personnel.
Encouragement for designing e-government systems of such complex structure, in dealing with technical and organizational challenges, and especially with securely exchanging personal or confidential information, has been boosted by certain outcomes of major European Commission (EC) projects. Software platforms are available since the year 2016, when e-AUthentication (e-AU), e-SIGNature (e-SIGN) and e-IDentification (e-ID) were publicly presented to Member States (MS)of the European Union (EU) [46-53]. In parallel to these developments, advances in Cloud Computing and Smart Cross Border e-Government (SCBeG) systems [41], [43] present alternatives in designing systems offering services to citizens in cross border environments. Also, existing autonomous systems, aiming to offer e-government services within territorial limits, are now updated for expanding business frontiers or/and facilitating the legitimate movement of citizens between the EU MSs [44].
In this work, we focus on a primary health care service offered by health care organizations to citizens looking for immediate treatment -at any time or place- he or she may be of need**.** The conceptual design of the proposed service will be based on the safety and authenticity precautions directed by Cloud Computing and the existing software platforms such as those provided by the European project STORK [46-53]. It should be capable of meeting the requirements of any European citizen for primary health care help anywhere within the EU [1, 17, 20, 65]. Apart from the Europeans, the service should also cover primary health care needs of any eligible citizen, like legal refugees while in mobility within the EU. Utilization of such a service should overcome problems related to the unavailability of a person's requirement for urgent

medical attention [55]. In such cases, systems can share a patient's digital record with authorized health care providers.
Focusing on the areas of security and privacy, our research group has tested the performance of existing platforms [53] under eIDAS[1] (Electronic IDentification, Authentication and trust Services) regulation by implementing a limited scale prototype which observes all current security requirements and standards .The implemented system supports an e-gov service concerning Erasmus student mobility and student certificates issuance [28]. The target audience of this system comprises mostly young citizens of Europe moving from one Member State to another, for higher education studies. This service also supports exchange of documents and certificates of graduates moving across Europe for studies or looking for a job. Systems requirements regarding safety and integrity were completely met [28].

The development of e-gov services involving cross-border transactions and using eIDAS authentication platforms, are usually hindered due to the lack of reliable implementation of eIDAS nodes by all EU member States and the rest of European countries. Expecting that this obstacle will be bypassed in the near future, we have proceeded to our system's conceptual design, using a case study of two European countries. In both of these primary health care services aim at developing systems that meet the main goal of providing services capable of supporting health care requirements during citizen mobility across Europe. Consciously, we have selected Greece and U.K. Greece, because is a member State already using eIDAS tools and with the political will to fully develop and use such systems. The U.K., because its National Health Service (NHS) is facing internal challenges in medical record sharing. The U.K. is trying to homogenize the practice of four primary health care systems across four legal entities in the country (England, Wales, Scotland and North Ireland). And this problem must be solved before or simultaneously to any consideration of a cross border service in support of mobility to its citizens. Apart, of this observation, the study of primary health care services of the above couple of countries has revealed a number of important issues needed to be addressed before any steps to be taken towards their e-gov automation. Since these issues may be common as well to other countries willing to join in the future, we have heavily elaborated on them and present in this work briefly.
Apart from the general concept and design requirements of the proposed e-government primary health care service, we also focus on the implementation of a module being the kernel of supporting systems. This module has been proposed as a deliverable of the project YGEIA1 [63] and is fully implemented and used by the Greek e-Government service for Social Security [23]. It is actually an extended citizen's medical file, the so called *Patient's Medical Protocol* (PMP). PMPs containing fully authenticated, medical information and further documentary evidence (diagnostic tests, hospital treatment reports, etc), through STORK platforms. A PMP should be the basic entity of the appropriate data base developed and kept by each European State on a central or distributed form. The PMP should be companion of any citizen, ready to be used and updated by especially authorized medical personnel of linked to the system health care organizations.

[1]EU regulation on a set of standards for electronic identification and trusted services for electronic transactions in the European Single Market. Introduced by EU Regulation 910/2014 of 23 July 2014 on electronic identification, repealing Directive 1999/93 / EC of 13 December 1999. It entered into force on 17 September 2014 and is effective from 1 July 2016 except for some of its specific provisions contained in Article 52.

Conclusively, the contribution of the present work to the effort to design and implement an e-government service capable of ensuring complete and effective diagnosis and treatment of migrant citizens, within the borders of a multinational territory, such as the EU, is as follows:

(a) Provide the most appropriate support system design model.
(b) Indicate the structure of the system and the step-by-step procedure for the detailed design and implementation of such a difficult and multidimensional project.
(c) Identify and demonstrate the obstacles to its successful implementation.
(d) Determine the technical specifications and advantages of the available platform from the EU.
(e) Focus the attention of all players (detailed system designers, software developers and implementers of the project), especially in the areas of data integrity, data security, privacy and legal requirements of the MSs in order for the service to ensure the security and confidentiality of personal data of the citizens who use it.
(f) Encourage further research and projects by EU Member States on the adoption of the STORK platform and the simplification, homogenization and safe opening of national primary health care services to the adoption of smart cross-border e-gov applications.
(g) Fully apply and conform with "The General Data Protection Regulation (GDPR)", the new EU Data Privacy Law[2].

The structure of the paper is as follows. In section 2 we present the functional organization of the primary health care service provided in Greece by a typical Primary Health Care Centre. A similar analysis of the NHS of U.K. in order to discuss practice, plans and challenges is following in the same section which is completed with the description of the appropriate network infrastructure of primary health care centers enabling the provision of relevant services to citizens in mobility. Section 3 presents the architecture, functionality and implementation requirements of a Smart Cross Border e-Gov (SCBeG) system and its structure, in the form of Decision Support System (DSS). Section 4, addresses implementation issues of cross border e-Government systems and the application of a European Primary Health Care e-gov service. Finally, section 5 provides a discussion with suggestions for further expanding this work, in the hope of inspiring further ideas, discussions and implementations.

2 Primary Health Care Organization

2.1 Primary Health Care Services

Primary Health Care in most of the EU Member States is usually provided by Local Community Health Centers (LCHC). LCHCs function under the umbrella of integrated National Public Health Care (NPHC) systems. In absence of LCHC's services, or complementary to them, private enterprises, such as Diagnostic Centers (DCs) fill the gap in certain areas. [63].

In all cases, following primary care provision locally, patients are either referred to secondary and tertiary care based on an initial diagnosis or released to their homes. A *"front-office primary health care service"*, is used to decide who the appropriate

[2] The new EU Data Privacy Law (GDPR) came into effect by the European Commission since 25th of May 2018. In time due, all MS will adopt its regulations to their legal systems and create a coherent data protection framework improving data protection and privacy rights.

addressee is by checking his/her identity verifying data. Such a system should forward the patient's medical record and file to the point of referral. Recently, a Greek initiative aiming at automating the front-office service offered so far to patients by the administration of LCHCs manually [63] had been proposed. In parallel, the Greek e-Government of Social Security Service [23] has proceeded to its implementation. The resulting simple e-government service has alleviated administrative burden on both administration and patients and has accelerated the decision process of the actors, leading to the final outcome (diagnosis, treatment or guidance for help outside the LCHC) more efficiently. The service suggests to patients the selection of the appropriate specialist, arranges the appointment with based on availability and carries out the necessary transfer of the patient's medical record. There are a number of legal and technical issues to be carefully considered here, such as access to medical records, their updating by eligible persons, and the capability of DCs to directly upload examination results to a patient's medical file.
The implementation of this *e-Government front-office primary health care service* has been in use in Greece for the past three years with satisfactory results [23].

2.1.1 Primary Health Care Services organization in Greece

During the past decade, the Greek health system has undergone a radical transformation. Having initially focused on implementing structural reforms to increase efficiency and reduce costs, more recent efforts have focused on establishing and strengthening systems supporting enhanced results [5].
There is now full health insurance coverage for all residents in Greece. The country is currently focused in addressing weaknesses such as excessive pharmaceutical costs, inefficiency of public procurement and inadequate primary care [4], [24].
The Greek health system is characterized as mixed, in terms of the supply of health services, and it follows the Beveridge model [2], with the provision of hospital care by public hospitals and the out-of-hospital care by Local Community Health Centres (LCHC). In terms of the demand for health services, it follows the Bismarck model [60], with the existence of social security funds [40]. At present, all health organizations (LCHC, DC, hospitals, etc.), amounting to 201 LCHCs, 168 Diagnostic Centers, 125 Public Hospitals and 1.487 regional health centers in rural areas are operate within the National Public Health Care (NPHC) system [21][62].
Continuous government reforms had not yet yielded the desired results, mainly due to a lack of necessary political will, limited resources, inadequate planning and significant challenges to the national health system over the past decade. [6]. Despite such challenges,and the most recent onslaught of the Covid-19 pandemic [21], the Greek Health System is now showing improved efficiency[59]. According to the Euro Health Consumer Index 2018 report, the Greek National Health System was in 29th place, showing an improvement of 4 positions, compared to the previous 5 years [61][62].
Information and Communication Technologies (ICT) and e-government systems have made a beneficial contribution to the health sector. In recent years, e-health in Greece has eliminated bureaucratic barriers, providing improved access to medical care, constantly available and up-to-date medical data in the Electronic Medical Record (EMR) and connection of remote LCHCs with large hospitals for medical data transfer to health professionals [60].

Cross-border health co-operation contributes to access of cross-border health systems [43]. European Initiatives aiming to enhance access to quality care in urban and rural border areas, encouraging joint use of medical services, have created the need for development of national and international mobility and patient rights legislation [42]. Under the European INTERREG program, four Cross-Border Public LCHCs, located in the prefectures of Ioannina, Florina, Serres and Evros collaborate in cross-border interoperability with the respective LCHCs of neighboring European countries [56].

2.1.2 Primary Health Care Services organisation in U.K.

Although the UK has recently left the European Union, patient records and their management are still subject to legislation that is compliant to that of the EU. Although the National Health System (NHS)appears as a single organisation, operationally and managerially it is a collection of different Health Care Authorities or Trusts. Each trust oversees the provision of healthcare across a specific geographic location, including hospitals and other care facilities, such as mental health care. Authorities are managed under different health care budgets depending on which part of the U.K. the authority lies, England, Scotland, Wales, or Northern Ireland. Patient record management varies according to the health trust to which the care facility belongs.

Although the content of patient records **is** dictated by the central NHS authorities, the implementation of such electronic records across the different trusts varies. Systems used to create and manage records vary considerably not just among different health care entities such as hospitals, but across different sections and departments of the same hospital. One should add that general practitioners, individual doctors or small health centres, which work with the NHS often, have different patient record systems, which might not be directly compatible with those of the hospitals in the same health care trust. This situation presents a considerable challenge of lack of interoperability that can severely affect the sharing of patient records within the country and the wider structure of the NHS. The organization has embarked a number of initiatives promoting interoperability across the different Health Care Trusts [30].

The NHS accepts that current models of care rely on the need for more effective information sharing between care settings, organisations and geographies. Doing so is reliant on the ability of IT systems across health and care to be interoperable with one another.

Since 2015 the NHS has developed clear guidelines as to the desirable interoperability of new systems and the requirements of contracting the development and management of new information systems as well as integrating legacy systems to the new structures.

These are outlined as seven priority areas:

1. NHS number/Citizen ID – real-time access to the NHS Number at the point of care across the service, ensuring that the NHS Number is associated with care record elements e.g. lab tests.
2. Medications – all medication messages in the NHS to be interoperable and machine readable across the service.
3. Staff ID – ensuring that there is a consistent way to identify and authenticate staff across the service.

4. Dates and scheduling – a consistent set of interoperability standards for dates and scheduling information that enables a consistent approach to appointment booking across venues of care and the creation of historic and forward views of appointments.
5. Basic observations – a consistent set of interoperability standards for the sharing of a core set of structured observations.
6. Basic pathology – a consistent set of interoperability standards for the sharing of a core set of pathology tests.
7. Diagnostic coding – implementation of SNOMED CT across the wider service, for Secondary Care, Acute Care, Mental Health, Community systems, Dentistry and other systems used in the direct management of care of an individual must use SNOMED CT as the clinical terminology.

The NHS interoperability strategy is based upon the following key building blocks [26]:

- Ensuring adoption of the NHS Number as the primary identifier when sharing information.
- Establishing regional interoperability communities to deliver their integrated digital care record solutions.
- Enabling open interfaces within and between integrated digital care records (IDCRs) to facilitate access to care information from local systems through open and standard interfaces.
- Prioritising the uptake of fundamental digital standards as ratified by the NHS England Board, such as NHS Number, Transfers of Care and SNOMED, to provide the basis for effective information sharing between different care settings and across locally and nationally delivered solutions.
- Creating a national patient record locator service to complement regional and local indices. This would act as a national index to support users wishing to locate and retrieve the records that exist for a patient/citizen using Open APIs from local and national care record solutions, (such as the Summary Care Record).

U.K. citizens, under the NHS, may have multiple detailed records or documents held on local systems, e.g. there may be a mental health record for a person at a particular trust or there may be other shared care records such as a maternity record or a healthy child record. The National Record Locator Service will, in due course, hold the links to the person's records that reside in multiple different systems. The core information standard does not define all these possible links.

The guidelines above have led to the undertaking of various initiatives to create collaborations across different health care providers and further across neighboring trusts in integrating and sharing patient records [31]. These initiatives, called Local Health and Care Record Exemplars, with one of the most prominent among such initiatives being Connecting Care in the West of England. Connecting Care is a digital care record system for sharing information in Bristol, North Somerset and South Gloucestershire. It allows instant, secure access to health and social care records for the professionals involved in your care.

This record contains some of the information held at GP practices, hospital departments, community services, mental health trusts, out-of-hours services and local authorities across the area covered. This information combines into a single, shared digital record all about each individual and can only be viewed in Connecting Care for

as long as it is held by the organisation it originates from. All health and social care organisations that share information in Connecting Care have to comply with the relevant laws about information retention [3]. Connecting Care is only accessible via the NHS broadband network. Individual user access is dependent on a professional's work role – their role defines which information they see. A user has to be authorised to have a Connecting Care account and each user is issued with a unique username and password. Only those directly involved with a person's care and authorised to use the system can see a specific individual's information. This could be a limitation in sharing records on a cross-border basis. Health and social care professionals have been using the Connecting Care integrated digital care record since 2013.

In exploring the interoperability of health systems across Europe, Larrucea et al [27] use the U.K. as an example in a case scenario exchanging patient records with other European countries over an interoperability enabled network. What these authors are proposing is not currently feasible, but could be operational once all the interoperability plans are in place in the near future. They present the Open NCP platform [18] as the backbone for exchanging patient's health records across European countries.

The European Commission has been supporting research and developing for providing a common network and an infrastructure to connect different national healthcare systems supports the above platform. The level of interoperability required in joining such an infrastructure is currently beyond the status in the UK and possibly other countries that have started their digitization of heath records early and many of them might depend on legacy systems. The OpenNCP can work well with the system proposed in this paper, which complements the OpenNCP by filling in its technical gaps in areas such as security and user authentication [15].

2.2 Networking Primary Health Care Services

Here we present the design of the appropriate network infrastructure of primary health care centers so that they will provide corresponding services to citizens in mobility. According to such G2C service, when a resident of a European of Member State (MS) A, is moving to MS B, they will be offered health care services more efficiently if their medical file is available to authorized personnel [42]. Steps followed are shown in Fig. 1 where:

- Any authorized user of the **MS A** can access a protected resource (medical file) from the **MS B** through the NPHC system.
- The system forwards the request to the Cross-Border Authentication System.
- If the authentication is valid then the medical file of the specific individual is accessed in the **MS B** NPHC system.
- Upon completion, the updated medical file is sent to the **MS A's** authorized user.

During the early stages of implementing the *e-Government front-office primary health care service* described in section 2.1, the ability to support patient mobility to a different EU country or, even elsewhere in the world was considered [43]. Security issues, national legislation, health care ethics, and systems interoperability are some of the more serious concerns. The introduction and adoption of the GDPR into national legislation alleviates some of such concerns. As the analysis of the digital patient record systems of two distinctively different countries showed, there is a need

to overcome serious interoperability issues to allow effective cross border medical record sharing. Cloud computing incorporation could adequately help in alleviating these [42, 65].

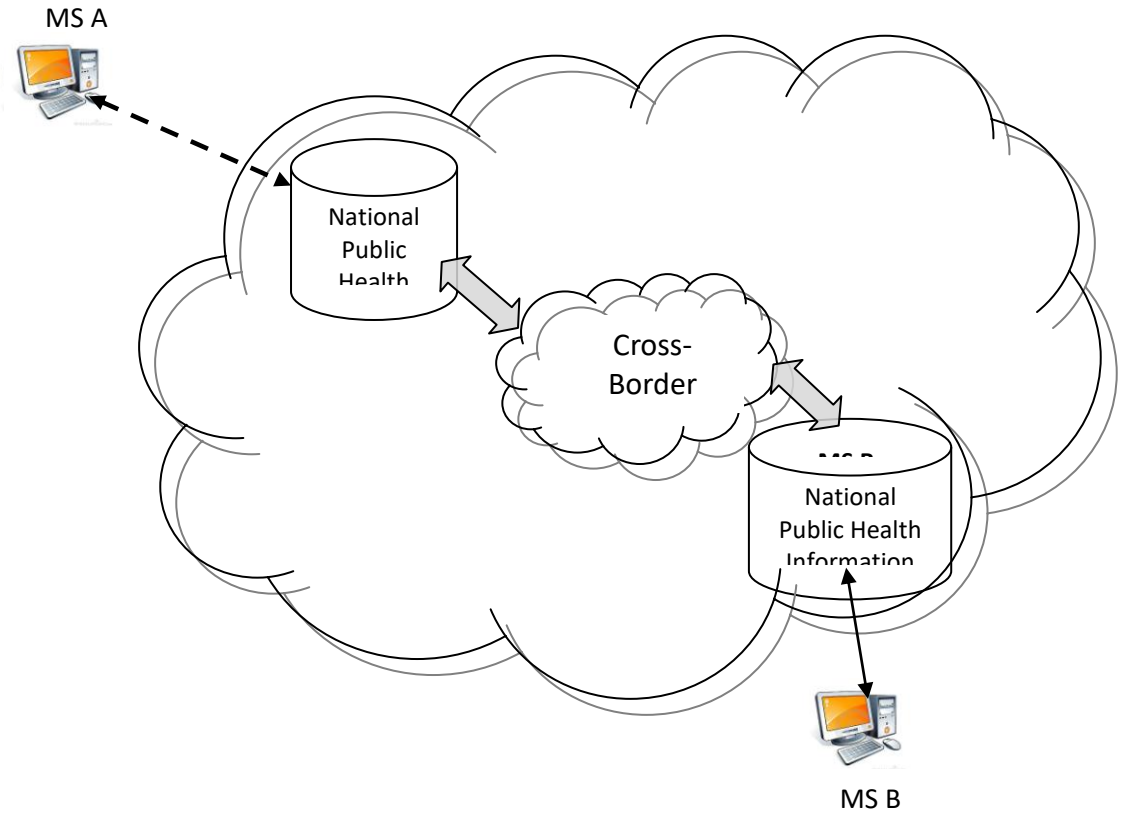

Fig. 1. Medical File Authentication Process in Primary Health Care Services

2.3 Mobility services through Smart Cross-Border e-Gov Systems

Security and privacy are key enablers of Smart Cross Border e-Gov systems while, one of their main objectives is to provide secure citizen mobility by utilizing state-of-the-art tools. Cloud Computing Privacy and Security techniques and models should be used by the relevant health care organizations [38, 54, 58, 64]. Certified authentication of diagnoses and medical documents or info of any form, included to Patient's Medical Protocol and issued by secondary and tertiary health care units, are online available when and if are required by eligible actors. These transactions are safely accompanying citizens, while they are moving across Member States, using the existing platforms on e-AU and e-SIGN, STORK 2.0 platforms. Thus, the proposed systems could significantly support the authorities, utilizing national e-IDs, under improved security measures and enhanced capabilities [42].
It should be emphasized that the design supports the use of the system, for any legitimate movements of citizens, including refugees, across Europe (decision of Heads of States or Governments, Summits of March the 7th and 18th, 2016, in Brussels) [7-13, 42]. Certification and authentication of medical data of refugees are of importance since a lot of cases of villains exploiting them have already been

reported (details of prerequisites and refugees legal movement are given in detail by Sideridis et al in [42].

3 The Smart Cross Border e-Gov model

3.1 The architecture

The Smart Cross Border e-Gov (SCBeG) system proposed here is actually an integrated Clinician Decision Support System (CDSS)comprising of three structural blocks: The I/O, the Validation-Authentication-Identification (VAI) and Processing blocks [26]. The whole authentication process, and part of the I/O block, is based on smart, machine learning, comparing, curing and checking data procedures. Machine Learning modules enable the proposed system to provide medical precision, where, utilizing and analyzing patients' medical data, they could, on the one hand, propose treatment protocols and, on the other hand, create machine learning models for predicting populations at risk from specific illnesses. Given the above, CDSS could have more decision-making data at its disposal. These smart items when added to the full decision-making process are enough to characterize a SCBeG system as a smart system based on clear decision-making methods, procedures and the cloud computing technology security capabilities. The proposed system could have significant impact in the improvement of the efficiency in delivering customized treatments based on a patient's medical history and increased healthcare delivery efficiency. Fig.2 shows a general functional diagram of the system. More specifically, the DSS accepts patient data as input and, taking into account patient clinical data, performs the required processes / routines and provides information about risk, treatment or follow-up as output.

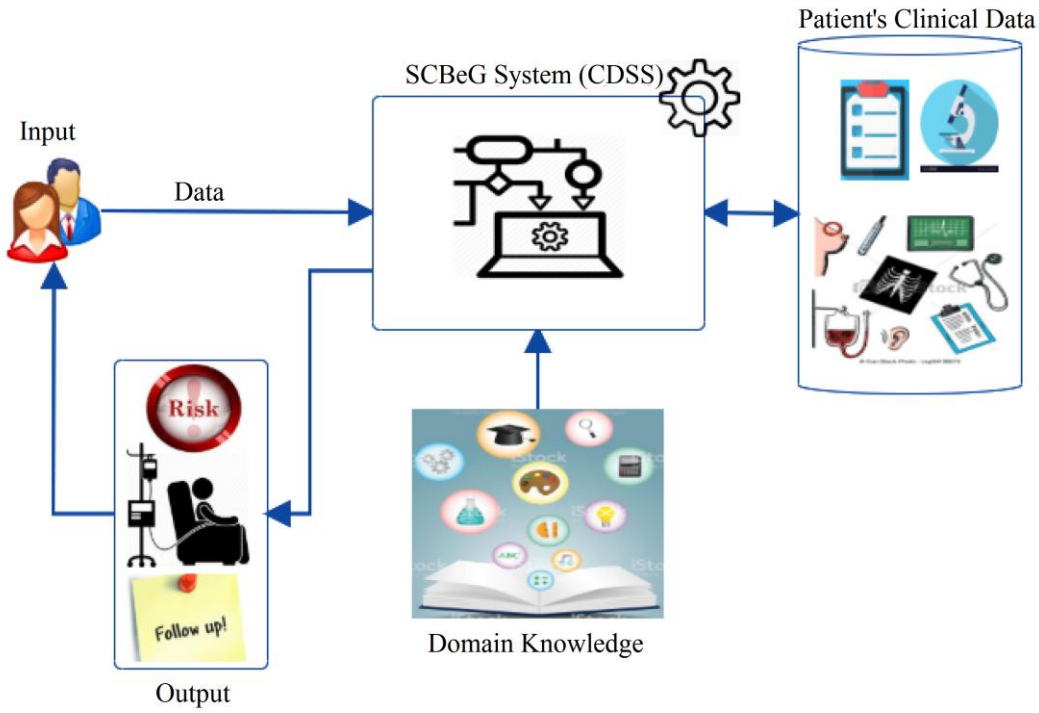

Fig 2. General diagram of the CDSS part of the SCBeG system

The VAI block provides additional capabilities in authenticating personal and sensitive data. A fundamental part of the VAI block comprises the platforms developed by STORK 2.0 project. These platforms include two identity verification models: The Pan-European Proxy Services (PEPS) &MiddleWare (MW) models (Fig. 3). It is noted that these models are based on established international standards, such as OASIS web SSO, ISO/IEC 27001, and OASIS DSS [43].

The authentication process is actually performed in two steps:
(a) Data submitted are validated using various validity tests and/with data available from original sources. In most cases, this is the most challenging step, since original sources may not be available or, if there are any, may be of questionable validity;
(b) Authentication is performed, among public/local agencies or any other local supervising organization of the service provided, both at citizen's State or enterprise's origin and the State in connection abroad. During this step, and in particular its Infrastructure as a Service (IaaS) model, should also be added to the system computer resources (software, hardware, servers) over the Internet. Public, local administrations and any third party are providers to the system. They should not only host the appropriate user's applications and personal files for testing but they should also handle maintenance, backup and upgrading services. Policy based services and automation of administrative tasks should also be main tasks of this IaaS.
The Processing block of the SCBeG system includes the appropriate Databases and a DSS mechanism while, two-way links exist with the VAI block. Subsequently, e-ID platforms and required programs facilitate Interoperability Solutions for European Public Administration (ISA), Connect European Facility (CEF) and guarantee availability of e-ID as a trust Service (IDaaS) [7-10]. Actually the European Commission, in an attempt to encourage Member States to extent their services with cross border functionalities, launched through the CEF program the Digital Single Web Portal, where all needed information on Building Blocks (BB) can be found. The service required is an e-ID of citizens, businesses (natural or legal persons) and public servants by authenticating themselves in order to be authorized and gain access to protected resources by verifying in a secure, reliable and trusted way their identity and/or their role. STORK1.0 provided the first e-ID BB while STORK2.0 extended it by demonstrating the capability of the provision of additional attributes by trusted Attribute Providers (AP). All the structural blocks of the above platforms, in combination with the appropriate BB of cloud computing, are strengthening and transform the proposed cross-border tool in an integrated SCBeG system.

3.2 The functionality

While STORK 1.0 & STORK 2.0 offered the first e-ID BB solution along with a software reference implementation, the European Commission covered the needs on legal interoperability by introducing the EU Regulation No 910/2014 of the European Parliament and the Council of the European Union [19-20]) on "Electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)" that repeals the Directive 1999/93/EC (Signature Directive). The Regulation, which has been adopted in July 2014 by the EU, provides the legislative and the regulatory framework for the creation of an appropriate environment, in which citizens, businesses and public administrations can interact securely, promoting and strengthening cross-border authentication. Key points of the Regulation are the mandatory cross-border recognition of the authentication schemes

of all the Member States in public administration services, the provision of trusted services without cost and the association of the already existing authentication schemes with pre-established assurance Levels of Authentication.
The regulation is also taking into account the STORK 1.0 & STORK 2.0 e-ID Interoperability Framework, established during the implementation of these projects. The framework consists of several national nodes acting as Pan-European Proxy Services (PEPS) or Middle Wares (MW Solution) depending on the architectural solution that has been followed by the Member States. The authentication request is further processed by the eIDAS proxy server, according to a specific Member State (MS) approach. Most countries follow the standard approach, in which a new authentication request is generated by the eIDAS proxy server and sent to the national IdP (National eID system part) (Fig. 3). [48, 52, 67]. The main objectives of these nodes are to conceal the complexity of the national systems and to be a link of confidence for the creation of a *Circle of Trust* in Europe. Such nodes have to guarantee scalability, since any change within a Member State should be transparent to the other Member States.

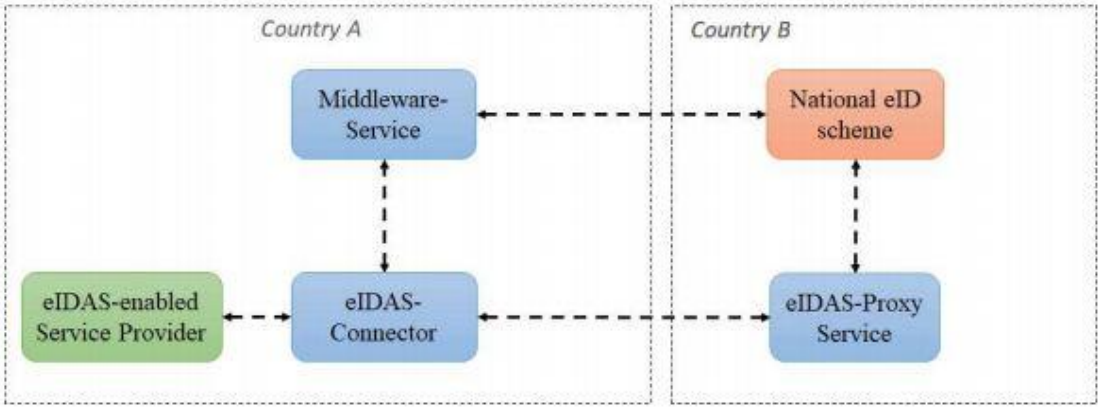

Fig 3. Electronic IDentification, Authentication, and trust Services (eIDAS) architecture [67]

The identification and authentication processes are based on message exchanging using the appropriate implementation profiles and technical specifications provided by STORK projects. The messages include personal and technical attributes. Details on the profiles, protocols and technical specifications used are beyond the scope of this paper and are omitted. By digitally signing the requesting and receiving assertions the requestor or sender are being authenticated, ensuring the integrity of the exchanged assertions.
Figure 4demonstrates a STORK 2.0 scenario where the user from MS A needs to be authenticated to a Service Provider (SP) established in MS B. PEPS architecture is followed by both the MSs. The MS where the SP is established and the MS of origin of the user. PEPS are acting, according specific scenarios, either as Citizen's PEPS (C-PEPS) or as Service PEPS (S-PEPS). In a number of cases, PEPS is acting as C-PEPS and S-PEPS also. In this scenario the PEPS of MS A is acting as C-PEPS while PEPS in MS B (service provider) as S-PEPS. The C-PEPS of MS A and the S-PEPS of MS B have a trusted relation by sharing their digital certificates. The same applies between S-PEPS and the SP.

The Service Provider supports cross border authentication through STORK 2.0 and provides the user with the ability to choose that option [43]. Users are authenticated through their national PEPS. Obviously, user's consent is required by PEPS before transferring his personal data to the SP. Thus, the whole authenticated process consent is in full compliance with the "Data Protection Directive" [14]. It may be cases requiring more than identity attributes. In such cases, users will be asked to choose the source of the attributes, authenticate again to the source, and give their final permission so that the process will be completed by the service provider.

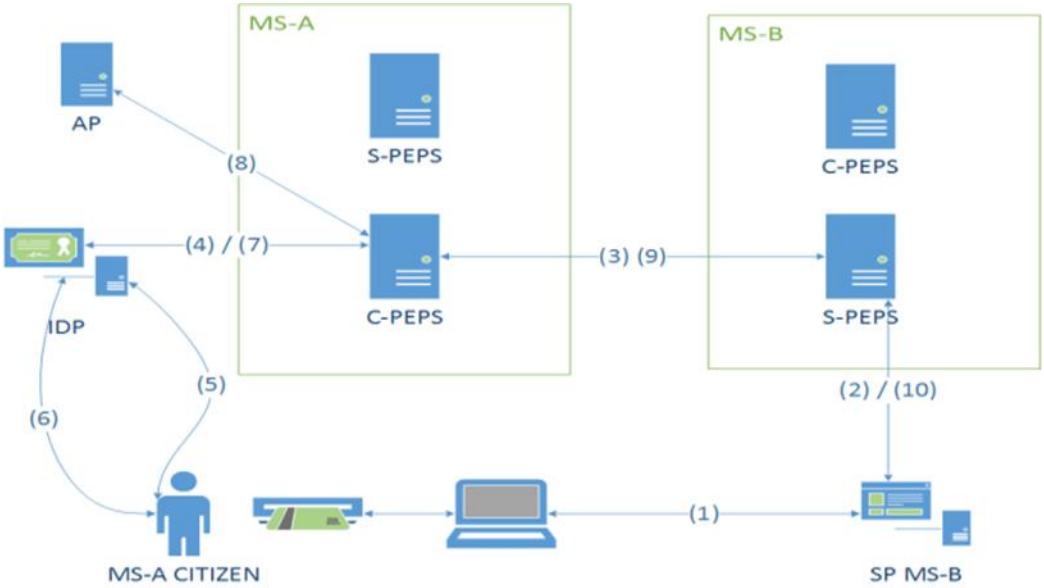

Fig 4. Cross Border Authentication through STORK 2.0 [50-51]

The authentication process can be completed following the 9 steps of Fig4[43]:

a. A safely protected resource of the SP is asked for access by the user A (1);
b. The outcome of the authentication process is sent by the SP to the corresponding S-PEPS (2);
c. The S-PEPS forwards the outcome of the authentication process to the relevant C-PEPS (3) of the Member State of origin of the user;
d. The authentication of the user takes place through C-PEPS to a national Identity Provider (IDP) (4,7);
e. Authentication of the user himself to the chosen IDP is taking place (5,6);
f. C-PEPS may retrieve (with the consent of the user) additional identification information or attributes from an AP (8);
g. Authenticated user's information and user's identification is transferred from the C-PEPS of Member State A to S-PEPS of Member State B (9);
h. S-PEPS forwards the information of step (7) to the service provider (10), see Fig. 2;
i. Access to the requested resource is permitted to the user.

4 Implementation issues of cross border e-Government systems

A major problem concerning the adoption of eIDAS authentication in cross-border transactions and applications is the lack of reliable implementation of eIDAS nodes

by all EU member states. Another problem providing obstacles in wide spread use of eIDAS authentication is the limited number of attributes supported by eIDAS regulation. This limitation forces the EU member States and the application developers to adopt specific solutions to overcome the absence of the desired attributes.

The universal implementation of Directive 2011/24 / EU on the implementation of patients' rights in cross-border healthcare by EU Member States has encountered various operational, legal and technical obstacles. The first barrier encountered by several countries is the pre-authorization requirement for time-consuming and costly treatments. This could be a major deterrent for countries with low health care budgets as percentage of their GDP Following the functional trades that arise in the full implementation of the European Directive, a patient, in order to be eligible for reimbursement, must have a referral or prescription from a doctor belonging to the National Health Fund (NHF) of the country of origin or a contracted EU doctor. In addition, the increasing complexity of the compensation process and the involvement of only 5 European Member States in the process [68], can be considered as the third barrier to access to cross-border healthcare.
Figure 5 below highlights a further challenge to integration. The map shows the number of different health care operators per country. This provides an even bleaker picture to that highlighted in section 2 that discussed the difference between two countries at the extreme opposites of such spectrum.

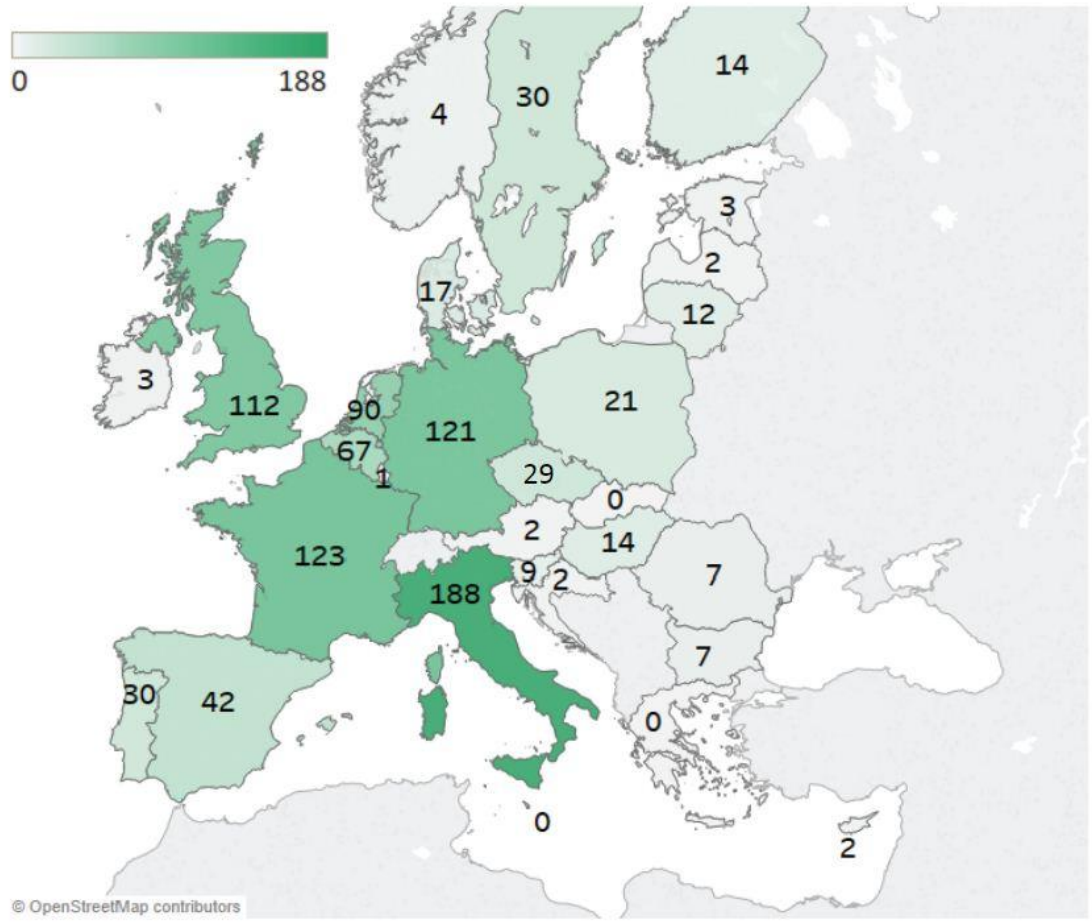

Fig 5. Distribution of healthcare provider members of European Reference Networks across the EU [66]

The use of eIDAS authentication can offer a system fully transparent to the user, supporting secure authentication and reduces the burden of bureaucracy. [28].
Indesigning such a service, many questions still remain unanswered and to answer them, a research community collective spirit is required. Many European standards are also needed and a lot of common problems to member States of the EU must be solved. For example, in any National Health System, medical personnel are authorized, under certain prerequisites, to access the medical record of a specific patient using his/her social security number. The problem arises when a physician of a European State needs to access the medical record of a citizen whose country of origin is another European State. Will he/she be allowed to update patients' records with new information (medical test results etc)? What about the different DB schemas of the various national DBs containing the health history of insured citizens of each Member State? Another problem concerns the diversity of the language in which the health history of each insured person is stored and the need of automatic translation to English. Natural Language Processing systems could be employed to convey the context and not merely a strict translation of medical notes inserted as free text in a patient's record.

In the context of seamless, secure and successful function of this cross-border system a risk management strategy must be adopted, taking into account a number of potentially critical risk factors. Statement of Work (SOW) and Work Breakdown Structure (WBS) should be drafted to avoid misunderstandings and creeps and it may be necessary to align the existing infrastructure of the EE States involved to incorporate the new features of the project outcome. Alongside, in Procurement Risks, the legal provisions in force in each country regarding healthcare should be taken into consideration. Finally, in Technology Risks, the maturity level of technical environment must be matched in order to be achieved the interoperability of the system, stakeholders actions must be taken to protect from obsolescence.[66].

5 Discussion - Conclusions

Integration and interconnection of national e-ID infrastructures, necessary for the type of systems proposed here, is still faced with reservation and remains an open issue despite the eight years that have passed since the first trials of implementation [55]. Although Austria had initially delivered a national e-ID system that could offer the basis of processing digital IDs from other countries and allow for the required transparency desirable in our proposal, new developments have brought more obstacles. Open European borders, increased legal and illegal migration, and changes in the laws handling personal data as directed by the GDPR, have intensified the need for additional security and complexity of the required systems.
Recently proposed e-government systems, combined with the results of the STORK 2.0 project, have contributed significantly to the implementation of innovative and reliable cross-border e-services, which have enhanced the daily life of European citizens, increased the transparency of electronic transactions, and ultimately contributed to the further development of the EU internal digital market. These e-government services, coupled with the latest emerging technologies, e.g. e-identification, are "equipped" with supplementary security protection to face a potential online attack for the loss of personal data. Despite the advance of such technologies the state of national health records needs further development for an

effective integration. The current pandemic has imposed and dictated a new ethic of collaboration across countries and this might help promoting a more urgent integration of cross border health care data management. Our proposal contributes a conceptual design that is realistic and capable of implementation under the current state-of-the-art technologies, communication, and security protocols.

Harmonization of digital systems supporting health care at national levels will enhance the effectiveness of cross-border systems. These have often been the subject of criticism as to their efficiency and transparency [36]. The continuous advances in technologies, the rapid integration of cloud, block chain, and artificial intelligence based solutions, are leading to the empowerment of such systems and can overcome questions of security and integrity. As the world is struggling to regroup in the wake of a massive medical emergency, and to fight against the continuous challenge of climate change, cross-border health systems will need to be made available sooner than expected. Although this work primarily references the European Union backed research efforts and novel results as the basis of the proposed system, the need and urgency is global.

EU backed research has laid the foundations at a technical level through the STORK project, its individual pilots, and similar systems have been proposed in the recent past. The important advantage of our proposed system is that the medical history of a patient will always be up to date and readily recoverable at any level of care (primary, secondary, or tertiary). The primary health care service can be quite demanding in its implementation, as there are too many legal aspects that still need to be taken into consideration and laboriously clarified. Medical data are predominantly sensitive and have often been a target of online attacks, reassurance of high level security of systems providing services of such a nature is always under very serious consideration. Blockchain enabled technologies will address such challenges effectively. The work is ongoing as systems such as the one proposed here are anthropocentric and as such will be presenting ever evolving and challenging requirements. Science will continue to address these as they evolve. The challenge is for the states and governments to support and finance such systems, so that the next pandemic can find the world more organized and more empowered to fight it.

References

1. Alguliyev, R., Yusifov, F.: Electronic Health as a Component of G2C Services. IJACSA, 8/3, 201-206 (2017)
2. Baldwin E. and Falkin C., Social Security Social Change: New Challenges to the Beveridge Model, Paperback, 1994
3. Connecting Care (2019) https://www.connectingcarebnssg.co.uk/ (accessed 31/08/2020)
4. Council of the European Union [online], Council Recommendation on the 2019 National Reform Programme of Greece, http://data.consilium.europa.eu/doc/document/ST-10161-2019-INIT/en/pdf (Accessed 06/08/2020)
5. Economou C., Kaitelidou D., Karanikolos M., Maresso A., Greece - Health system review, European Observatory, 2017
6. Economou M., The impact of the economic crisis in Greece: epidemiological perspective and community implications. In: Stylianidis S, eds. Social and Community Psychiatry:469–83.Springer, Cham, 2016

7. European Commission (a).: [online] http://ec.europa.eu/information_society /apps/projects/ (Accessed 23/04/2016)
8. European Commission (b).: [online] http://ec.europa.eu/digital-agenda/en/connecting-europe-facility/ (Accessed 17/04/2016)
9. European Commission (c).: [online] https://ec.europa.eu/dgs/connect/en/content/ electronic-identification-and-trust-services-eidas-regulatory-environment-and-beyond/ (Accessed 17/04 /2016)
10. European Commission (d).: [online] http://ec.europa.eu/isa/ (Accessed 17/04/2016)
11. European Commission, 2016a. [online] http://ec.europa.eu/digital-agenda/en/digital-agenda-europe-2020-strategy/ (Accessed 17/04/2016)
12. European Commission: The European eGovernment Action Plan 2011-2015- Harnessing ICT to promote smart, sustainable & innovative Government in ICT for Government and Public Services. In: EC publications, Brussels (2010a), http://eur-lex.europa.eu/legal-content/ EN/TXT /PDF/?uri=CELEX:52010DC0743&from=en/ (Accessed 22/04/2016)
13. European Commission: Towards interoperability for European public services. In: T.C. Communication from the Commission to the European Parliament, the European Economic and Social Committee and the Committee of the Regions, Brussels (2010b), http://ec.europa.eu/isa/documents/isa_iop_communication_en.pdf (Accessed 22/04/2016)
14. European Council (a).: [online] General Secretariat of the Council, EU International Summit, EU-Turkey Statement of the EU Heads of State or Government, Brussels (2016), http://www.consilium.europa.eu/en/press/ (Accessed 24/04/2016)
15. European Interoperability Framework For Pan-European eGovernment Services.: [online] Brussels, (2004), http://ec.europa.eu/idabc/servlets/Docd552.pdf?id=19529/ (Accessed 19/04/2017)
16. European Parliament and the Council of the European Union.: Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC 27. In: Official Journal of the European Union, L 257/73, Brussels (2014)
17. European Patients - Smart open Services, epSOS: [online] http://www.epsos.eu/ (Accessed 20/04/2016)
18. European Union (2019) OpenNCP Properties https://ec.europa.eu/cefdigital/wiki/ display/EHNCP/OpenNCP+properties (accessed 11/09/2020)
19. European Union.: A Common European Asylum System, Luxembourg: Publication Office, ISBN 978-92-79-34626-2
20. European Union: Directive 2011/24/eu of the European Parliament and of the Council on the application of patients' rights in cross-border healthcare. [online] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065: EN:PDF (Accessed 17/06/2017)
21. Georgakopoulou T., Ongoing measles outbreak in Greece related to the recent European-wide epidemic. Epidemiology & infection, 146 (13):1692–8, 2018

22. Höchtl, J., Polycek, P., Schölhammer, R.: Big Data in the Policy Cycle: Policy Decision Making in the Digital Era. Journal of Organizational Computing and Electronic Commerce, 25, No 4, 147-169 (2015)
23. IDIKA.: [online]http://www.idika.gr (in Greek), Accessed 29/06/2019)
24. IOBE, The pharmaceutical market in Greece: Facts & figures 2017. Hellenic Association of Pharmaceutical Companies, Athens, 2018
25. Janowski, T., Estenez, E., Baguma, R., Platform governance for sustainable development: Reshaping citizen - administration relationships in the digital age. Government Information Quarterly 35, iss. 4, 1-16 (2018). https://doi.org/10.1016/j.giq.2018.09.002
26. Kelsey, T. (2015) Digital Health Services by 2020: Delivering Interoperability at Point of Care to Support Safe, Effective, Efficient and High Quality Care, NHS England http://www.england.nhs.uk/wp-content/uploads/2015/03/item9-board-260315.pdf (accessed 11/09/2020)
27. Larrucea, X., Moffieb, M., Asafb, S., and Santamaria, I. (2020) Towards a GDPR compliant way to secure European cross border Healthcare Industry 4.0, Computer Standards & Interfaces 69 (2020)
28. Maliappis, M., Gerakos, K.,, Costopoulou, C., Ntaliani, M.: Authenticated academic services through eIDAS, International Journal of Electronic Governance (IJEG), Vol. 11, No. 3/4 (2019)
29. National Organization for the Provision of Healthcare Services, [online], Law 4213/2013 - Adaptation of national legislation to the provisions of Directive 2011/24 / EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (L 88/45/4.4.2011) and other provisions. https://www.taxheaven.gr /laws/law/index/law/565 (only available in Greek) Accessed 28/06/2017)
30. NHS (2018) How to access your health records https://www.nhs.uk/using-the-nhs/about-the-nhs/how-to-access-your-health-records/ (accessed 11/09/2020)
31. NHS (No Date) Digital transformation- Connected digital systems- Interoperability, https://www.england.nhs.uk/digitaltechnology/connecteddigitalsystems/interoperability/ (accessed 12/09/2020)
32. NHS England (2015) Interoperability Handbook, Health & Social Care Centre
33. Parycek, P., Höchtl, J., Ginner, M.: Open Government Data Implementation Evaluation. Journal of Theoretical and Applied Electronic Commerce Research, 9, No 2, 80-100 (2014)
34. Parycek, P., Rinnerbauer, B., Schossböck, J.: Democracy in the digital age: digital agora or dystopia. International Journal of Electronic Governance, 9, Nos 3/4, 185-209 (2017)
35. Parycek, P., Schossböck, J.: The unibrent movement. A successful case of mobilising lurkers in a public sphere. International Journal of Electronic Governance, 4, Nos 1/2, 43-68 (2011)
36. Pimenidis, E., Georgiadis, C.K.: Can e-Government Applications Contribute to Performance Improvement in Public Administration?. International Journal of Operations Research and Information Systems 5(1), 48-57 (2014)
37. Pimenidis, E., Iliadis, L.S., Georgiadis, C.K.: Can e-Government Systems Bridge the Digital Divide?. In: Proceedings of the 5th European Conference on Information Management and Evaluation (ECIME 2011), Dipartimento di Informatica e Comunicazione, Universitàdell'Insubria, 403-411, Como, Italy (2011)

38. Posch, K. C., Posch, R., Tauber, A., Zefferer, T., Zwattendorfer, B.: Secure Privacy - Preserving eGovernment Best Practice in Austria. Rainbow of Computer Science. 259-269 (2011)
39. Professional Record Standards Body (2019) CORE INFORMATION STANDARD IMPLEMENTATION GUIDANCE, https://theprsb.org/wp-content/uploads/2020/07/Core-Information-Standard-Implementation-Guidance-v1.3-.pdf (accessed 13/09/2020)
40. Reiter, A., Prünster, B., Zefferer, T.: Hybrid mobile edge computing: Unleashing the full potential of edge computing in mobile device use cases. In: Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing. 935-944 (2017)
41. Sideridis, A. B.: A Smart Cross Border e-Gov Primary Health Care Medical Service. Proceedings of the 8th E-Democracy Conference on: Safeguarding Democracy and Human Rights in the Digital Age. S. Katsikas and V. Zorkadis (Eds.), CCIS 1111, pp. 67–78, 2019
42. Sideridis, A. B., Pimenidis, E., Costopoulou, K., Yialouris, C. P., Savvas, I., Maliappis, M., Ntaliani, M., Karetsos, S., Tsiafoulis, S., Protopappas, L., Chatziandreou, A.: e-Gov: Recent Advances in Life Sciences & EE's Project Proposals (Medical, Animal, Plant, Food Sciences and Environmental Protection), Doctoral Consortium, HAICTA 2017. Chania, Crete (2017b)
43. Sideridis, A. B., Protopappas, L., Tsiafoulis, S., Pimenidis, E.: Smart Cross-Border e-Gov Systems and Applications. In: Proceedings of the 6th E-Democracy Conference. 151-168, Athens, Greece (2015)
44. Sideridis, A. B., Protopappas, L., Tsiafoulis, S., Pimenidis, E.: Smart Cross-Border e-Gov Systems: an application to refugee mobility. To appear in the International Journal of Electronic Governance (2017a)
45. Sideridis, A. B., Protopappas, L.: Recent ICT advances applied to smart e-government systems in Life Sciences: In: Proceedings of Information and Communication Technologies in Agriculture, Food and Environment. 7th HAICTA. Kavalla, Greece (2015)
46. Sideridis, A. B., Protopappas, L.: Citizens Safe Mobility Necessitate the Implementation of a Primary Health Care E-Gov Service: The Case of the Europeans. BJSTR, Vol. 33(3), pp. 25859-25861 (2021)
47. STORK 1.0 (a). [online] https://www.eid-stork.eu/ (Accessed 20/04/2016)
48. STORK 1.0 (b) [online] eID Consortium, D2.3 Quality authenticator schem. http://www.eid-stork.eu/ (Accessed 22/04/2016)
49. STORK 1.0 (c) eID Consortium, D 3.2.1 SAML. [online] http://www.eid-stork.eu/ (Accessed 22/04/2016)
50. STORK 2.0 (a). [online] https://www.eid-stork2.eu/ (Accessed 12/04/2016)
51. STORK 2.0 (c). [online] https://www.eid-stork2.eu/ (Accessed 20/04/2016)
52. STORK 2.0 (d) eID Consortium, D4.3 First Version of Technical Design. [online] https://www.eidstork2.eu/ (Accessed 22/04/2016)
53. STORK 2.0. (b), [online] https://www.eidstork2.eu/images/stories/documents/ETSI%202015 %20presentation%20-STORK%202.0.pdf/ (Accessed 14/04/2016)
54. Stranacher, K., Krnjic, V., Zefferer, T.: Trust and reliability of public sector data. In: Proceedings of World Academy of Science, Engineering and Technology (WASET). 384-396 (2013)

55. Tauber, A., Zefferer, T., Zwattendorfer, B.: Approaching the Challenge of eID Interoperability: An Austrian Perspective. European Journal of ePractice, 14, 22-39 (2012)
56. Vasileiou, I., Giannopoulos, A., Klonaris. C., Vlasis, K., Marinos, S., Koutsonasios, I., Katsargyris, A., Konstantopoulos, K., Karamoutsos, C., Tsitsikas, & A., Marinos, G., The potential role of primary care in the management of common ear, nose or throat disorders. Quality in Primary Care,17(2), 145–148, 2009
57. Viale Pereira G., Cunha, M. A., Lampoltshammer, T., Polycek, P., Testa, M. G.: Increasing collaboration and participation in smart city governance: a cross case analysis of smart city initiatives. Information Technology for Development 23, No 3, 526-553 (2017)
58. Viale Pereira, G., Polycek, P., Falco, E., Kleinhans, R.: Smart governance in the context of smart cities: A literature review. Information Policy 23, No 2, 143-162 (2018)
59. Wallace Lorraine S., A View of Health Care Around the World, Annals of Family Medicine Journal, 2013
60. WHO Regional Office for Europe, Monitoring and documenting systemic and health effects of health reforms in Greece, Copenhagen, 2019
61. WHO, European Health for All Database [online]. Retrieved from https://gateway .euro.who.int/en/datasets/european-healthfor-all-database/(Accessed 12/08/2020)
62. Yfantopoulos J., Chantzaras A., Drug policy in Greece. Value in Health Regional Issues, 16:66–73, 2018
63. Yialouris, C. P., Chatziandreou, A., Implementing YGEIA1. TR/258, InfoLab, AUA (2017), (in Greek), Athens, Greece, 2017
64. Zefferer, T.: Mobile Government: e-Government for mobile societies. Stocktaking of current trends and initiatives. Vienna Secure Information Technology Center, 14, 1-58 (2011)
65. Zwattendorfer, B., Zefferer, T., Stranacher, K.: An overview of Cloud and Identity Management Models. WEBIST, 1, 82-92 (2014)
66. Aziz, L. & Cooke, H. (2005). Risk Management in Healthcare Information Technology (HIT) Projects. Paper presented at PMI® Global Congress 2005—North America, Toronto, Ontario, Canada. Newtown Square, PA: Project Management Institute.
67. Berbecaru Diana, Lioy Antonio, Cameroni Cesare (2019), Electronic Identification for Universities: Building Cross-Border Services Based on the eIDAS Infrastructure, MDPI
68. Kowalska-BobkoIwona, Mokrzycka Anna, Sagan Anna, Włodarczyk W. Cezary, Zabdyr-JamrózMichał (2016), Implementation of the cross-border healthcare directive in Poland: How not to encourage patients to seek care abroad? Elsevier