Cross-Border e-Government Authentication Services

Alexandros B. Sideridis[(1)], Elias Pimenidis[(2)], Konstantina Costopoulou[(1)], Costas P. Yialouris[(1)] Maria Ntaliani[(1)], Ioannis Savvas[(3)], Michael Maliappis[(1)], Sotiris Karetsos[(1)], Stergios Tsiafoulis[(4)], Loucas Protopappas[(1)], Andreas Chatziandreou[(5)]

[(1)]AUA, GR, {as, tina, yialouris, michael, ntaliani, karetsos, lprotopappas}@aua.gr
[(2)]UWE, UK, elias.pimenidis@uwe.ac.uk
[(3)]Admin of Macedonia-Thrace, GR, jsav@aua.gr
[(4)]ydmed, GR, s. tsiafoulis@dmed.gov.gr
[(5)]UoP, GR, xatziandreoy@gmail.com

Abstract. Recent advances in technology have made possible the implementation of e-Government services to citizens, businesses and public agencies, facilitating cross-border transactions and necessitating the transfer of confidential and personal data. Such services require the efficient validation of data through authentication. Recently, the European Commission provided to the Authorities of Member States the appropriate regulation and systems for cross-border transactions. Literature review shows that there is an increasing interest in such systems for health, social services, agriculture, and life sciences in general. This article proposes cross-border authentication services through three specific case studies. The eminency of the respective services mainly lies to the fact that they are secure, easy-to-use and authenticated, circulating confidential and personal data, through public agencies of European member states. These services use cloud computing technology fighting the incompatibility of diverge environments and thus facilitating the provision of primary health care services, the mobility of European citizens and legitimate refugees and the authentication of agricultural farmers around the European Union.

Keywords: e-Government systems, Authentication, Electronic Identification, Cloud Computing, Health Care, Refugees' Mobility, Farmers.

1 Introduction

Few decades ago, Information and Communication Technology (ICT) complex applications have been implemented to eliminate manual work in areas of continued globalization, such as e-commerce, e-banking, e-health, e-justice, e-forensics and e-crime. The availability of e-government mixed (automated and manual) models, capable of meeting complex requirements (e.g. security), extended global research activity to new areas, such as e-agriculture, e-environment, e-forestry, and logistics. Benefited stakeholders include public agencies, food companies, agricultural organizations and enterprises, farmers, and citizens and businesses in general. Recently, innovative e-government applications are aiming to fully automate public services by removing administrative burdens and improving time response from

Proceedings of the 8th International Conference on Information and Communication Technologies in Agriculture, Food and Environment (HAICTA 2017), Chania, Greece, 21-24 September, 2017.

Government to Citizens (G2C) and Government to Business (G2B). Automation, integrity and time efficiency of relative services, necessitate the implementation of supporting administrative Government to Government (G2G) services necessary for the implementation of the previously mentioned G2C and G2B services.

Recently, e-government systems had already come at an unpresentenced rate. Sideridis et al. (2015) state that national and local governments need further integration of e-government systems for "*enhancing citizens' daily activities and creating the appropriate basis in public administrations for the development of knowledge based economies*". ICT innovations, like cloud computing, Big Data and Internet of Things (IoT), were incorporated to the appropriate structures of complex e-government systems, extending existing e-government services, or designing new ones. Developments through European Commission (EC) projects have made possible the use of secure, easy-to-use and authenticated e-transactions exchanging confidential and personal data in urgent activities, such as citizens' mobility and products logistics and transportation. To this end, since October 2016, developed platforms of e-AUthentication (e-AU), e-SIGNature (e-SIGN) and e-IDentification (e-ID) were publicly available to Member States of the European Union (EU) [STORK 1.0 (a,b,c), 2016 and STORK 2.0 (a,b,c), 2016]. Based on these platforms, Sideridis and Protopappas (2015) have proposed e-government services using cloud-computing technology to support Smart Cross Border e-Government (SCBeG) systems. Using SCBeG systems is a promising solution for the secure exchange of sensitive data among public agencies, businesses and citizens for cross-border G2C, G2B and G2G services. Also, latest developments in SCBeG systems encourage further research and attention for the implementation of the appropriate models and services of direct and immediate need. Such case is the development of systems for expanding business frontiers or/and facilitating legitimate movement of citizens between the EU Member States (Sideridis et al., 2017).

In this article, three indicative examples are proposed from health, social and agricultural sectors. Specifically, the first example illustrated supports health services capable of meeting the requirements of any European citizen (European Union, 2011), (European Patients, 2016) crying for primary health care help and treatment's arrangement, as he/she is moving around the EU, regardless his/her state of origin. Due to the very sensitive nature of personal health data, medical records, files and information regarding specific examinations and tests, SCBeG system should be based on high level security e-AU, e-SIGN and e-ID platforms, such as those provided by the European project STORK. Thus, e-government primary health care services will be provided to any citizen of the EU during his mobility to any Member State without the obstacle of the unavailability of his medical files. The importance of such services is evident, particularly in cases of emergency and need of immediate medical attention (Tauber et al., 2012).

The second example presented in this paper aims to support services of legitimate mobility of non- European citizens to the Member States of the EU. In particular, the main G2C service, provided by the SCBeG system, concerns refugees' mobility, i.e. to the effective management of the movement of thousands of Syrian and Iraqi refugees across Europe. This service allows accurate registration of refugees, data

authentication and their identification for any future movement across the EU according to the decision of Heads of States or Governments in the relevant Summits of March the 7th and 18th, 2016, in Brussels (European Council a, 2016). At the same time, refugees' identification will allow them to be issued a work permit and to establish themselves legally in accordance to the 1951 Geneva Convention relating to the Status of Refugees, their rights and the legal obligations of Member States. This problem necessitates immediate action and therefore, the proposed in this paper SCBeG system is of immense urgency and importance.

The third example describes farmers' cross-border authentication services. Recently, an EU pilot for authentication services to farmers has estimated that digital certificates for farmers could save 400 hours a year in time needed to complete the application, and that such services can reduce cross-border administrative burdens for farmers and public agencies (G2B and G2C), provide easy digital access to a wide spectrum of documents and services, simplify login process for foreign farmers, as well as reduce time, effort and cost for foreign users (e-SENS, 2017a; 2017b). Also, authentication services, can contribute to the agri-market integration across Member States, since the EU agri-food sector is quite problematic regarding cross-border barriers for trading, due to food quality and safety. In this context, an agricultural e-service authentication process concerning EU farmers is described.

The structure of the paper is as follows. Section 2 describes the three examples for authenticating cross-border electronic transactions in health, social services and agriculture. In section 3, the architecture, functionality and implementation of the SCBeG system is presented. This system supports the implementation of the services proposed in the aforementioned examples. Discussion follows in section 4 where, at the same time, an attempt is made to encourage researchers to participate in similar projects and stimulate further ideas, discussions and implementations.

2 Application Areas

2.1 Primary Health Care Services

Primary Health Care in most of the EU Member States is usually provided by Local Community Health Centres (LCHC). The medical personnel of a LCHC usually employs general practitioners as family doctors and, in most of the cases, specialists covering the basic medical doctor's specialties. LCHCs are functioning under the umbrella of integrated National Public Health Care (NPHC) systems. In absence of LCHC's services, or even if complementary to them, private enterprises, usually called Diagnostic Centres (DCs) are filling the gap (a DC is consisting of a number of medical doctors of the basic specialties forming a consortium). In urban areas and cities patients are usually directly addressing to Outpatient Departments or, in case of emergency, the Emergency Units of nearby Hospitals. All health organizations (LCHCs, DCs, hospitals etc.) are accommodated under the umbrella of the respective NPHC system.

In all cases above, by this first aid step health service provision, patients are locally treated or guided to secondary and tertiary care in accordance with a diagnosis made by health professionals of the above units. Patients are so addressed in allied health professions chiropractic, physicians, physician associates, dentistry, midwifery, nursing, medicine, optometry, pharmacy, psychology etc. Prior and during the actual patient's guidance, a *"front-office primary health care service"*, apart from being capable to decide who the appropriate addressee is by checking his social security number and verifying identity data, it should also provide to him patient's medical record and file. Then, the specialist, or any health advisor acting as the addressee, should be able to properly advice, treat or redirect his/her patient as appropriate.

Recently, a Greek initiative aiming at automating the front-office service offered so far to patients by the administration of LCHCs manually (Yialouris and Chatziandreou, 2017) has been established. This initiative implements a simple e-government service alleviating administrative burden of both administration and patient, and accelerating the decision process of the actors (patient-administrator-specialist) and the final outcome (diagnosis, treatment or guidance for help outside the LCHC). In other words, the service under development suggests to patients the selection of the appropriate specialist arranges the appointment with him/her in accordance to his/her availability and carries out the necessary transfer of patient's medical record. There is a number of legal and technical issues to be carefully considered, like the proper consideration of medical record's upgrading by eligible persons, as well as the capability of DCs to directly upload to patient's medical file their examination results.

The implementation of the above described *e-Government front-office primary health care service* to patients looking for a proper advice and treatment in LCHC or any other similar organization, is expected to be ready and put into practice, for a pilot period of six months, by spring, 2018. In summary, according to this G2C service, when a European citizen or any other legitimate person of Member State A or MS A, is moving to MS B, should be offered health care services in a more efficient and direct way while his medical file will be available to authorised personnel. 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.
- Consequently, the medical file is sent to the **MS A's** authorized user.

During the first stages of implementing the *e-Government front-office primary health care service* described above, a question was raised with regard to system's commitment to provide such a service in case of a patient's mobility to a different EU country or, even if elsewhere, than that of his/her own state of origin. SCBeG systems providing such services seem to present the appropriate basis in also dealing with *"cross-border front-office primary health care services"* of a kind such that described above (Sideridis et al., 2015). Security issues and strict national law with regard medical record's sensitive personal data, authentication of data, final patient's

identification and more general interoperability problems are very effort consuming problems under serious consideration. Obviously, e-government services necessitating merge of heterogeneous computer environments, as those of different states needed to cooperate in offering primary health care services to European citizens moving around the EU, will face difficult interoperability problems. Cloud computing incorporation will elevate and adequately help (Sideridis et al., 2017).

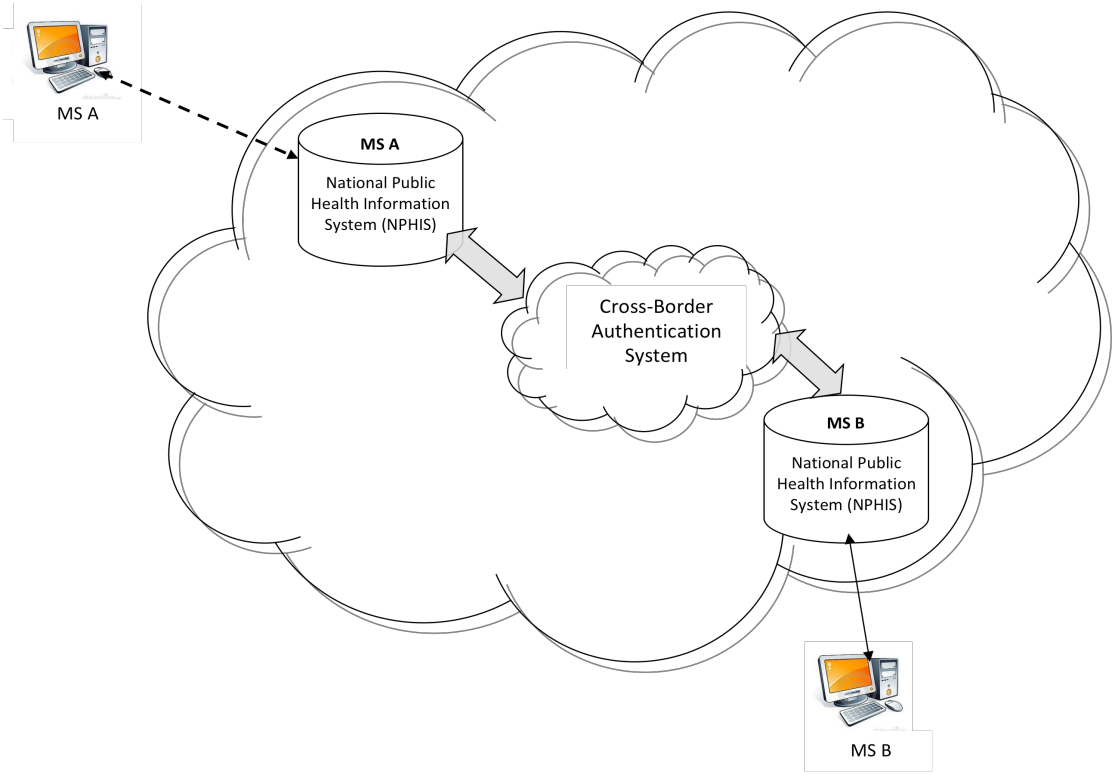

Fig. 1 Medical File Authentication Process in Primary Health Care

2.2 Mobility services

Security and privacy are key enablers of SCBeG systems while one of their main objectives is to provide secure citizen mobility by utilizing state-of-the-art tools and models to deliver a safe environment for transactions and movement across EU member states using the existing platforms on e-AU and e-SIGN. STORK 2.0 has implemented successfully e-ID. Thus, the proposed systems could significantly support the authorities, utilizing national e-IDs, to monitor the transactions of any

citizen and authorized personnel, under improved security measures and enhanced capabilities of Cloud Computing (Sideridis et al., 2017).

Recently, efforts are made in creating interoperable environments and satisfying requirements for G2G, G2B and/or B2B models of operation. Respective applications will mostly benefit Small and Medium Enterprises (SME) and this will contribute to combat unemployment (free movement of young people without the burden of bureaucratic restrictions and full use of e-ID). Similar systems strengthen the foundation of the authors' proposal for the implementation of an e-government system to support the effective management of legitimate movement of thousands of Syrian and Iraqi refugees across Europe, entitled "REfugees MObility e-Government" (REMOGO) system (Sideridis et al., 2017). Services offered by REMOGO allow accurate registration of refugees, data authentication and their identification for any future movement between the EU countries according to the decision of Heads of States or Governments in the relevant Summits of March the 7th and 18th, 2016, in Brussels (European Commission a, 2016). At the same time, authentic refugee's identification will allow them to be issued a work permit and to establish themselves legally. This problem necessitates immediate action and therefore, the proposed SCBeG system is of immense urgency and importance. Figure 2 illustrates the authentication process of a refugee using the REMOGO system.

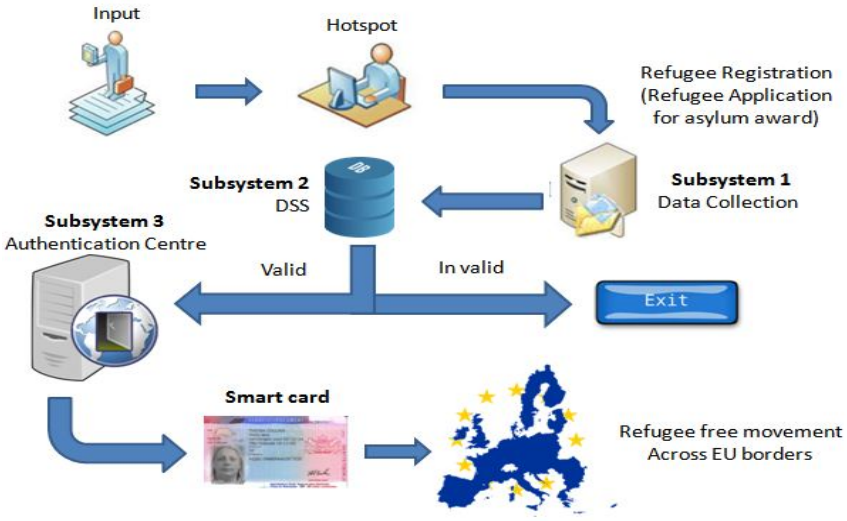

Fig. 2 Authentication Process by REMOGO system

In general, SCBeG systems will be able to capture, analyze and authenticate cost effectively, constantly changing (due to mobility) data, just in time with streaming computing. Confidence should be built in the ability to integrate, understand, manage and govern these massive data, stored in various devices and public organizations across the globe, in a proper way throughout its lifecycle. Big Data platforms fit better than any other platform available for the management and processes of such data. Certain limitations resulting from the use of Big Data, like the five key

elements of Big Data platforms used (high volume, high velocity, high variety, high complexity and high variability) should be dealt with the use of certain smart efficiency tests of capture analysis, data curation, sharing etc.

2.3 Farmers' Authentication Services

The increased demand for high-quality, safe, and eco-friendly products comprises a great challenge for the food industry that activates in a dynamic, globalized and complex supply chain environment. Till today, full transparency has not been achieved for cross-border and global food supply chains, where it is vital for stakeholders (e.g. farmers) and consumers to be able to have access to consistent, complete, accurate and timely food quality tracking and tracing information (Xu et al., 2014). EU is the world's largest exporter of food and drink products, the second largest importer, and the leading exporter of processed agricultural products. Still, the EU food and drink industry faces problems in the supply chain regarding transparency, lack of attractiveness for skilled workers and low market integration across member states. (European Commission, 2017a; 2017b). Specially, according to Egan and Guimarães (2017) the agri-food sector is the most problematic regarding cross-border barriers for trade, resulting from national differences concerning food quality and safety among Member States. In particular, Italy, France, Germany, and Greece account for 64 percent of the barriers in the agri-food sector. Seamless authentication is one of EU priorities for improving cross-border interoperability. In order to ensure cross-border mobility, transparency and visibility, which are critical to ensure food safety and quality, cross-border authentication services for farmers are proposed.

In particular, this example describes a process for the authentication of EU farmers, who wish to log in foreign agricultural public agency portals. This can be achieved using the eIDAS approach (Lenz and Zwattendorfer, 2016). Specifically, the main objective of the proposed process is the connection of a farmer from MS A to MS B for accessing an online service (e.g. applying for subsidy, registration of cattle). Steps followed are shown in Fig. 3 where:

- The farmer visits the agricultural e-service web portal and tries to log in using eIDAS credentials acquired from MS A (1).
- The agricultural e-service web portal redirects the farmer to his/her national eIDAS node, through the local eIDAS node for authentication (2,3).
- The national eIDAS node accepts farmer's credentials and returns to the agricultural e-service web portal the required attributes (4).
- The agricultural e-service web portal allows farmer access to digital services (5).

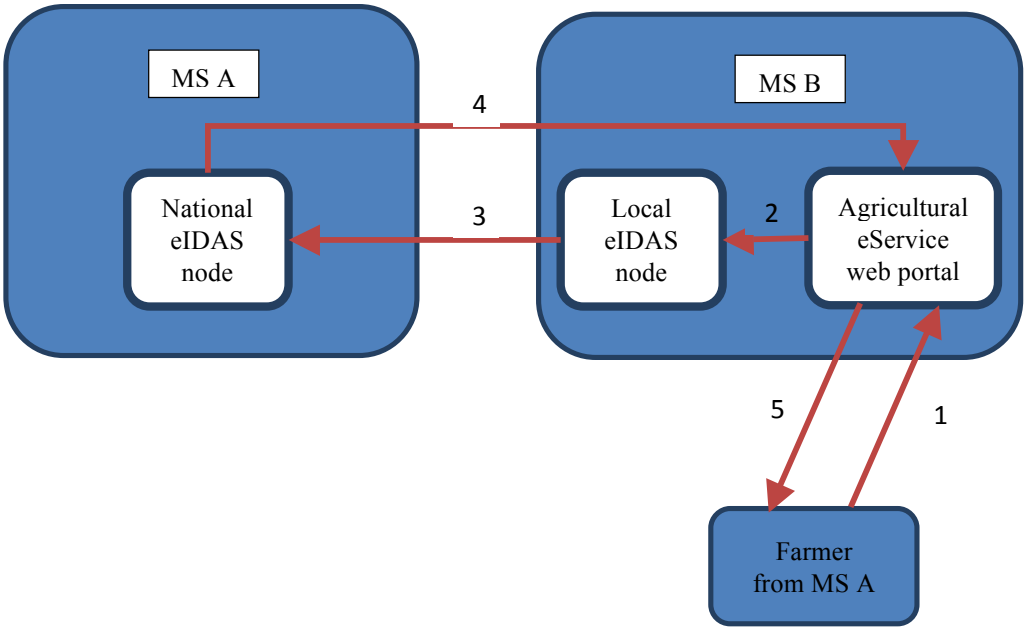

Fig. 3 Agricultural e-service web portal authentication process

3 The SCBeG model

3.1 The architecture

A SCBeG system is actually a Decision Support System (DSS) comprising of three structural blocks: The I/O, the Validation-Authentication-Identification (VAI) and Processing blocks. The whole authentication process, and part of the I/O block, is based on smart, machine learning, comparing, curing and checking data procedures. These smart items 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 and Big Data. The VAI block provides additional capabilities in authenticating personal and sensitive data. Obviously, a fundamental part of the VAI block consists of the platforms developed by STORK 2.0 project. These platforms include two identity models: The Pan-European Proxy Services (PEPS) & MiddleWare (MW) models (Fig. 4). It is noted that these models are based on established international standards, such as OASIS web SSO, ISO/IEC 27001, and OASIS DSS (Sideridis et al., 2017).

The authentication process is actually performed in two steps:

(a) Data submitted are collected by the system using various validity tests and/with data available from original sources. In most cases, this is the most difficult 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 organisation 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 programmes facilitate Interoperability Solutions for European Public Administration (ISA), Connect European Facility (CEF) and guarantee availability of e-ID as a trust Service (IDaaS) (European Commission a,b,c,d) 2016]. Actually the EC, in an attempt to encourage Member States to extent their services with cross border functionalities, launched through the CEF programme 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 and Big Data, 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 EC covered the needs on legal interoperability by introducing the EU Regulation No 910/2014 (European Parliament and the Council of the European Union, 2014a) 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 (LoA). For the

determination of the LoA of an electronic authentication scheme, organizational and technical aspects of the authentication procedure are taken into account. These concern both the phases of registration and of the online authentication process that compose the authentication scheme. Table 1 describes the four-scaled STORK Quality Assurance Authentication (QAA) levels have been considered on the determination of the eIDAS LoA. Every transaction shall make available, on request, the user's level of quality of the authentication in order to enable each Services Provider to decide whether the conditions are met, so as to provide the electronic service.

Table 1. STORK QAA / eIDAS LoA

STORK QAA levels	***eIDAS***	***Description***
1	*-*	*No or little credibility*
2	*Low*	*Low reliability*
3	*Substantial*	*An important credibility*
4	*High*	*High reliability*

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 is consisting of several national nodes acting as Pan-European Proxy Services (PEPS) or MiddleWares (MW Solution - VIDP) depending on the architectural solution that has been followed by the MSs (STORK 1.0 b; STORK 2.0 c). 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. Moreover, these nodes have to guarantee scalability, since any change within a member state should be transparent to the other member states.

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 4 demonstrates a STORK 2.0 scenario where the user from MS A needs to be authenticated to a Service Provider (SP) established in MS B. In this scenario, both the MSs where the SP is established and the MS of origin of the user, use PEPS architecture. In accordance with specific scenarios PEPS could act as Citizen's PEPS (C-PEPS) or as Service PEPS (S-PEPS). In a domestic use case 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 SP supports cross border authentication through STORK 2.0 and provides the user with the ability to choose that option. The user authenticates himself through

his national PEPS. PEPS always ask for the user's consent before transferring his personal data to the SP. The consent is asked so as the authentication process to be in compliance with the "Data Protection Directive" (European Parliament and the Council of the European Union, 2014a). If more than identity attributes are needed, the user will be asked to choose the source of the attributes, in some cases authenticate again to the source, and give his explicit permission to relay them to the service provider.

The authentication process is as follows:

- The user wishes to access a protected resource of the SP (1);
- The SP forwards the outcome of the authentication process to the corresponding S-PEPS (2);
- The S-PEPS forwards the outcome of the authentication process to the relevant C-PEPS (3) of the country of origin of the user;
- The authentication of the user takes place through C-PEPS to a national Identity Provider (IDP) (4,7);
- User authenticates himself to the chosen IDP (5,6);
- C-PEPS may retrieve (with the consent of the user) additional identification information or attributes from an AP (8);
- User authentication and identification information is transferred from the C-PEPS of country A to S-PEPS of country B (9) with the consent of the user;
- Finally, S-PEPS forwards this information to the service provider (10);
- The user has access to the requested resource.

The procedure is the same in case of using eIDAS nodes instead of PEPS ones.

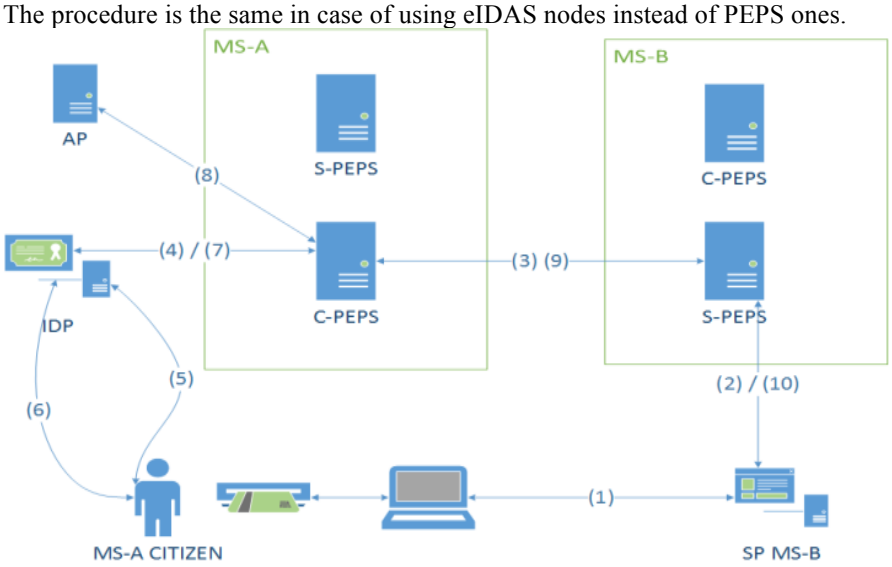

Fig. 4 Cross Border Authentication through STORK 2.0

Cross border authentication is expected to increase the effectiveness of public and private online services, e-transportation, e-logistics, e-business and e-commerce in the EU.

4 Discussion

Integration and connection of national e-ID infrastructures, necessary for the type of systems like those proposed recently is still faced with reservation and remains an open issue although five years (Tauber et al., 2012) have passed already since their first trial of implementation. Actually, it was Austria's first attempt to take the challenge to deploy national e-ID modules in online processes by creating the legal basis for acceptance of foreign e-ID. This attempt has proved to be very successful and has managed, during its deployment, to satisfy several national legal requirements, which had to be taken into account. By now, according to the Austrian law, foreign citizens are registered in the so-called supplementary register by the means of qualified certificates and are treated equally like local residents. A similar approach using direct registries merge rather than creating supplementary ones has been adopted in this work.

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 enhance the improvement of the daily life of European citizens, increase the transparency of electronic transactions and ultimately contribute to the further development of the EU internal market. These e-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.

It is obvious that full implementation of the above systems is still a difficult task. Still, they will bring many benefits in key areas, such as health, social services and agriculture. Although they have often been so far criticized for their poor contribution to efficiency and transparency in service provision (Pimenidis and Georgiadis, 2014; Pimenidis et al., 2011), recent advances promise successful implementation results. The proposed applications like the cross-border primary health care system can fill the gap in cross-border environment when a European citizen moves among the EU Member States and needs immediate health care. The need to improve the way of health care delivery and the recovery of the medical history of the patient is critical, as any possible delays in the delivery of the required treatment can be disastrous. Although the EU has laid the foundations at a technical level through the STORK project and its individual pilots, and similar systems appear a few years back, 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 and 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 account and must reassure a high level of safety as medical data are predominantly sensitive and have often been a target of online attacks.

Given the urgency of the business situations and daily life events presented in the three indicative cases, the previous experience and the state of the art technologies available from existing research outputs and extensive pilot studies by EU, research groups are encouraged to join in and actively participate in numerous EU programmes.

References

1. CEF building blocks. [online] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+building+blocks/ (Accessed 21/04/2016).
2. Egan, M., and Guimarães, M. H. (2017) The Single Market: Trade Barriers and Trade Remedies. JCMS: Journal of Common Market Studies, 55: 294–311. doi: 10.1111/jcms.12461.
3. e-SENS, 2017a. E-Agriculture. [online] https://www.esens.eu/content/e-agriculture
4. e-SENS, 2017b. White Paper D3.8 Overall e-SENS business case. https://www.esens.eu/sites/default/files/e-sens_d3.8_white_paper.pdf
5. European Council (a), General Secretariat of the Council, EU International Summit (2016), EU-Turkey Statement of the EU Heads of State or Government. [online] http://www.consilium.europa.eu/en/press/ (Accessed 24/04/2016).
6. European Commission (2017a). Food and drink industry. https://ec.europa.eu/growth/sectors/food_en
7. European Commission (2017b). Processed agricultural products in the EU. https://ec.europa.eu/growth/sectors/food/processed-agricultural-products/trade-overview_en
8. European Commission (a). [online] http://ec.europa.eu/information_society/apps/projects/ (Accessed 23/04/2016).
9. European Commission (b). [online] http://ec.europa.eu/digital-agenda/en/connecting-euro pe-facility/ (Accessed 17/04/2016).
10. 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).
11. European Commission (d). [online] http://ec.europa.eu/isa/ (Accessed 17/04/2016).
12. European Commission, 2016a. [online] http://ec.europa.eu/digital-agenda/en/digital-agenda-europe-2020-strategy/ (Accessed 17/04/2016).
13. European Commission, 2010a, The European eGovernment Action Plan 2011-2015-Harnessing ICT to promote smart, sustainable & innovative Government in ICT for Goverment and Public Services 2010. Brussels: EC publications. http://eur-lex.europa.eu/legal-content/EN/TXT /PDF/?uri=CELEX:52010DC0743&from=en/ (Accessed 22/04/2016).
14. European Commission, 2010b, Towards interoperability for European public services. Brussels: T.C. Communication from the Commission to the European Parliament, the European Economic and Social Committee and the Committee

of the Regions. http://ec.europa.eu/isa/documents/isa_iop_communication_en.pdf (Accessed 22/04/2016).
15. European Interoperability Framework For Pan-European eGovernment Services, 2004: Belgium. [online] http://ec.europa.eu/idabc/servlets/Docd552.pdf?id=19529/ (Accessed 19/04/2017).
16. European Parliament and the Council of the European Union, (2014a), 'Regulation (EU) No 910/2014 Of the European Parliament and Of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC 27, Official Journal of the European Union, L 257/73.
17. European Patients - Smart open Services, epSOS, [online] http://www.epsos.eu/ (Accessed 20/04/2016).
18. European Union (b), A Common European Asylum System, Luxembourg: Publication Office, ISBN 978-92-79-34626-2.
19. European Union, (2011), 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).
20. Lenz, T., & Zwattendorfer, B. (2016). Towards Cross-Border Authorization in European eID Federations. In Trustcom/BigDataSE/I SPA, 2016 IEEE (pp. 426-434). IEEE.
21. Ministry of Health, (2008), Law 3655/2008 - Administrative and organisational reform of the Social Security System and other insurance-related provisions. [online] http://www.etaa.gr/files/N.3655-08.pdf (only available in Greek) Accessed 29/06/2017)
22. National Organization for the Provision of Healthcare Services, (2013), 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. [online] https://www.taxheaven.gr/laws/law/index/law/565 (only available in Greek) Accessed 28/06/2017)
23. Pimenidis, E. and Georgiadis C.K. (2014) Can e-Government Applications Contribute to Performance Improvement in Public Administration?, International Journal of Operations Research and Information Systems, 5(1), 48-57.
24. Pimenidis, E., Iliadis L.S. and Georgiadis C.K. (2011) 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, Università dell'Insubria, Como, Italy, 8-9 September 2011, pp. 403–411.
25. Sideridis A. B., Protopappas L., (2015) Recent ICT advances applied to smart e-government systems in Life Sciences: Information and Communication

Technologies in Agriculture, Food and Environment. 7th HAICTA 2015 International Conference, Kavala.
26. Sideridis A. B., Protopappas L., Tsiafoulis S. and Pimenidis E., (2015) Smart Cross-Border e-Gov Systems and Applications, Proceedings of the 6th E-Democracy Conference (e-Democracy 2015), Athens, Greece, 10-11 December 2015, pp. 151-168.
27. Sideridis A. B., Protopappas L., Tsiafoulis S. and Pimenidis E., (2017) Smart Cross-Border e-Gov Systems: an application to refugee mobility", to appear in the International Journal of Electronic Governance.
28. STORK 1.0 (a). [online] https://www.eid-stork.eu/ (Accessed 20/04/2017).
29. STORK 1.0 (b) eID Consortium, D2.3 Quality authenticator schem. [online] http://www.eid-stork.eu/ (Accessed 22/04/2016).
30. STORK 1.0 (c) eID Consortium, D 3.2.1 SAML. [online] http://www.eid-stork.eu/ (Accessed 22/04/2016).
31. STORK 2.0 (a). [online] https://www.eid-stork2.eu/ (Accessed 12/04/2016).
32. STORK 2.0. (b), [online] https://www.eidstork2.eu/images/stories/documents/ETSI%202015%20presentation%20-STORK%202.0.pdf/ (Accessed 14/04/2016).
33. STORK 2.0 (c). [online] https://www.eid-stork2.eu/ (Accessed 20/04/2016).
34. STORK 2.0 (d) eID Consortium, D4.3 First Version of Technical Design. [online] https://www.eidstork2.eu/ (Accessed 22/04/2016).
35. Tauber A., Zefferer T., Zwattendorfer B., (2012) Approaching the Challenge of eID Interoperability: An Austrian Perspective, European Journal of ePractice, No 14, pp. 22-39.
36. Xu, F. J., Zhao, V. P., Shan, L., & Huang, C. (2014). A Framework for Developing Social Networks Enabling Systems to Enhance the Transparency and Visibility of Cross-border Food Supply Chains. GSTF Journal on Computing (JoC), 3(4), 132.
37. Yialouris and Chatziandreou, 2017. Implementing YGEIA1. TR/258, InfoLab, AUA(2017), (in Greek).