Smart Cross-Border e-Gov Systems: an application to refugee mobility

Alexander B. Sideridis[1], Loucas Protopappas[1], Stergios Tsiafoulis[2] and Elias Pimenidis[3]
[1] Informatics Laboratory, Agricultural University of Athens
{ as, loucas.protopappas}@ aua.gr
[2] Hellenic Ministry of Interior- Administrative Reconstruction and e-Governance
stetsiafoulis@gmail.com
[3] University of the West of England, UK
Elias.Pimenidis@uwe.ac.uk

Abstract. Smart Cross-Border e-Government Systems for citizens and business have been recently proposed to further improve everyday lives, expand business frontiers, and facilitate the movement of citizens by reducing the constraints imposed by existing borders between federal states. Their main advantage is their ability to be used by governmental organizations, citizens, and business, in a cross border environment, thanks to the availability of recently developed electronic authentication, identification and signature platforms. These latest technological advances may contribute to solving the mobility issue of legitimate refugees in various European countries. This problem has at the time of writing evolved into a major crisis due to the mass movement of hundreds of thousands of Syrian and Iraqi refugees across Europe and requires immediate attention. An implementation of Smart Cross-Border e-Government Systems appears to be a very good option in supporting the management of individuals and their movement in order to address this crisis.

Keywords: E-Government, Smart Cross-Border e-Government Services, Internet of Things, Cloud Computing, refugee mobility, eIDAS, e-Identification

1 Introduction

Since the turn of the twenty first century, developments in e-Government systems have come at an unprecentended rate. New models of e-Government systems have been continuously proposed in an effort to meet the need for integrated e-Government services, in both enhancing citizens' daily activities and creating the appropriate basis in public administrations for the development of knowledge based economies. In the past few years, advanced Information and Communication Technologies (ICT) innovations like Cloud Computing, Big Data and Internet of Things were incorporated to the appropriate structures of complex e-Government systems, extending existing e-Government provisions, or enabling the design of new ones, aiming to cover wide application areas. Such systems can be further extended in an authenticated global environment to cover needs for services beyond national borders and national economies in a global spectrum (Sideridis, 2013; Sideridis and Protopappas, 2015; Sideridis et al., 2015). Lately, e-Government systems were enriched

by adding the dimension of intelligence to their structures so they could support special requirements like those dictated by expanding business frontiers or/and facilitating legitimate movement of citizens between member States of the European Union (Sideridis et al., 2015).

Industries or societal activities that have mostly benefited in an era of economic recession and continued globalization are those of e-Banking, e-Health, e-Justice, e-Forensics and e-Crime (combating international terrorism, fraud and crime). The availability of e-Government models capable of meeting complex requirements extended global research activity to new areas of primary concern including the so called "mild" areas, from the secure government systems point of view. Such areas include Life Sciences and their practices; in particular, e-Agriculture, e-Forestry, e-Environment, e-Food Sciences and Technologies. Thus, many applications of e-Government systems have been proposed to cover needs for example of primary agricultural production and the necessary export-import facilities for Small to Medium Enterprises (SMEs) in particular (Nielsen S., 2001). The latest applications contribute in removing the administrative burden from Government to Citizens (G2C) and Citizens to Citizens (C2C) models as well the necessity of supporting administrative Government to Government (G2G) procedures. In day-to-day activities the time factor is very important and the contribution of recent technological advances and availability of platforms in the areas of e-Authentication (eAU), e-Signature (e-SIGN) and e-Identification (eID) are significant in supporting successful and timely cross border bureaucratic transactions (Tauber. et al, 2012).

The complexity in modeling e-Government systems, due to the incorporation of the above mentioned ICT advances to existing platforms and procedures, is compensated by the provision of simple, efficient and reliable applications. The existence and widespread use of mobile devices offers a further supporting factor to the effort of integrating such services. A common characteristic of all these recently proposed systems is their cross-border capability, i.e. their support to C2C, G2C and G2G services employed between at least two states or countries. For reasons of taxonomy and taking into account the immense research activity in developing e-Government systems of fully exploiting and incorporating eAU, e-SIGN and eID platforms, mainly for cross border applications, these systems will be called Smart Cross-Border e-Gov systems (SCBeG) (Sideridis et al., 2015).

To effectively deal with cases requiring global security for cross border applications, national Governments of the European Union (EU) States are promoting further intergovernmental Administration to Administration (A2A) and G2G models to be implemented. At the same time, the EU has announced special programmes and supports projects for the development of cross board e-Government systems promoting interoperability and making full use of eAU, eID and eSIGN platforms. This initiative is part of the overall strategy of the EU aiming to the creation of a Digital Single Market in Europe (European Commission 2010a, European Commission 2010b, European Commission a, European Commission b). Of course, it is up to the national Governments to adopt the results and platforms just announced by the successful outcome of the EU project STORK 2.0. Obviously it will take some time for the establishment of SCBeG systems and applications to embrace security sensitive "tradi-

tional" e-Banking, e-Health, e-Justice e-Education and e-Customs (already in existence) systems.

The STORK 2.0 (STORK 2.0a) project that has been recently completed, and launched by the European Commission, incorporates all the latest emerging techniques (Biometrics Data Collection (BDC), IoT, CC, BD) and can tackle a large number of chronic or unprecedented problems. The key outputs of STORK 2.0 offer eID integrated and pioneered cross-border applications that allow citizens and SMEs to establish new e-relations across the EU borders (STORK 2.0b).

Security and privacy are key enablers of CBeG systems, particularly in the EU. One of the main objectives of such systems 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 states. In the wake of the recent intensity of international terrorism, an important question comes in mind: "Could the terrorist attacks of 2015 and 2016 in Paris and Brussels have been prevented with SCBeG systems making full use of eID and eAU?" Using the existing platforms on eID and eAU, STORK 2.0 has been implemented successfully; the proposed systems could significantly support the authorities utilizing national eID to monitor the transactions of any citizen or any SME.

In a recent paper (Sideridis et al., 2015), emphasis was given to the key objective of STORK 2.0 project in creating interoperable environments and including four cross-sectoral pilots satisfying requirements for Government, Government to Citizen, Government-to-Business and/or Business-to-Business modes of operation. Such applications will mostly benefit Small 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 eID) and the present economic recession (Sideridis and Protopappas, 2015). The idea of legitimate mobility of young people beyond the restriction of national borders, forms the foundation of the authors' proposal here for an e-Government model to enable the implementation of a service to support the effective management of the movement of thousands of Syrian and Iraqi refugees across Europe. This service will allow accurate registration of refugees, data authentication and their identification for any future movement between the European States 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; Emergency Response Coordination Centre). At the same time, authentic refugee's identification will allow them to enjoy 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 states. This problem necessitates immediate action and therefore, the proposed SCBeG system is of immense urgency and importance.

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 BD like the five key elements of BD 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.

SCBeG systems and their structure in general are described in section 2. The combination of the special facilities of e-Government systems of this type, with platforms available on eID are presented in section 3. A current proposal for a project aiming to develop a SCBeG system supporting the mobility of refugees is presented in section 4. A discussion and conclusions are given in sections 5 and 6 respectively.

2 Structure of SCBeG Systems

The SCBeG system is actually a Decision Support System (DSS) comprising three structural blocks: The I/O, the Validation-Authentication-Identification (VAI) and Processing blocks. The VAI block provides additional capabilities in authenticating personal data prior to a decision relating to the legitimate mobility of a refugee, during that person's mobility and after they have settled down to a European country in accordance with the specific EU settlement agreement.

Refugee's data collection of the I/O block is a time consuming, mostly bureaucratic process, during which data are painfully extracted by interviewing people or trying to get the appropriate information from documents of questionable validity. Personal Data will be managed (stored, authenticate and processed) to the benefit of the end user and primarily the refugees themselves. Therefore, the refugees' personal data will be safely stored and processed with strict confidentiality and under the provision of the user's consensus and Data Protection Authorities' approval. EU's and corresponding national government's legislation regarding this very sensitive issue will be an important subject for consideration of the REMOGO (Refugee Mobility Smart Cross Border e-Government) system analysis phase. Once personal data are collected, by any means, these data are imported to the system. The next step involves the authentication process actually performed in two sub steps: (a) Data collected are authenticated by the system using various validity tests and/with data available from original sources. This sub step is the most difficult one since, in most cases, no original sources will be available or, if they are, may be of questionable validity. (b) Authentication is performed during refugee's mobility among Public/Local Authorities Administrations so that permission can be issued for a final settlement of a refugee in accordance with the signed EU agreement. During this step Cloud Computing, 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 and Local Administrations are third party providers to the system. They should not only host the appropriate user's applications and personal data 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 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 of judging a user's legitimately in applying for free mobility and settlement are enough to characterize REMOGO as a smart system based on clear decision making methods, procedures and the already available CC and BD platforms.

In the recent past, the European Union has implemented a multi-level security framework (fig. 1) in order to ensure the security and reliability of services (STORK 2.0b). A significant element of the "Digital Agenda for Europe" is that of interoperability as it forms one of the seven pillars of the Europe 2020 Strategy which sets objectives for growth, security and development for the European Union (EU) by 2020 (Euractiv a,; European Commission, 2016a).

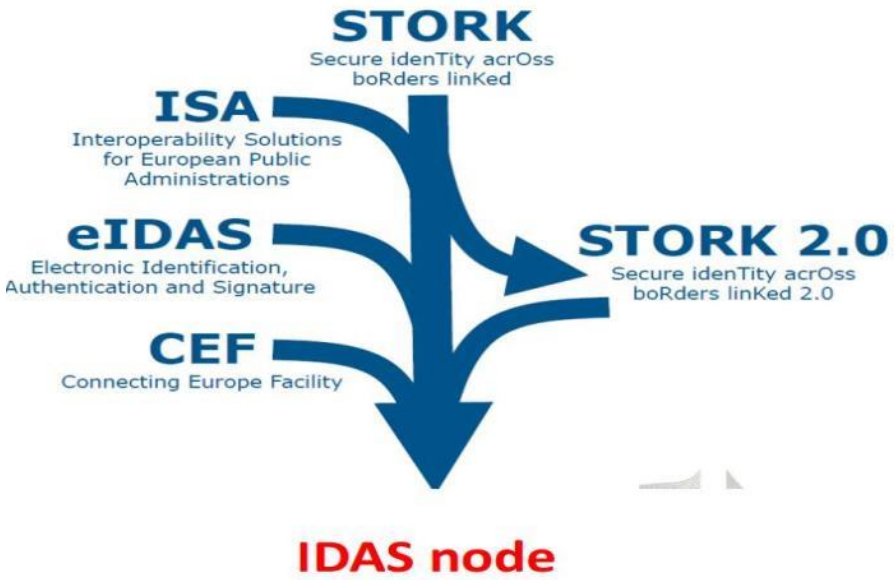

Fig. 1 IDAS node. Source: https://www.eid-stork2.eu

Part of the architecture of SCBeG systems is Subsystems, Databases and Decision Support System while links have been established among the others platforms and development programs; (Connecting Europe Facility (CEF), electronic IDentification and trust Services (IDAS), Interoperability Solution for European Public Administrations (ISA) (European Commission, 2016a; European Commission, 2016b; European Commission, 2016c; European Commission, 2016d).

The building blocks of the above platforms, in combination with the new emerging technologies (CC, BD, IoT and BDC) can strengthen and transform the existing cross - border systems in SCBeG, as new eAU, e-SIGN and EID platforms are offered to support them. A fundamental part of the operation and architecture of

the above systems is STORK 2.0, which is based on established listed international standards (OASIS web SSO, ISO/IEC 27001, OASIS DSS) and it consists of a combination of the following identity models (Pan-European Proxy Services (PEPS) & Middleware Model (MW) (Leitold, 2009). Additionally, all these provide eID authentication for diverse services providers, in combination with the next-generation techniques, such as CC. This architecture is called STORK VIDP, and is shown in figure 2 below.

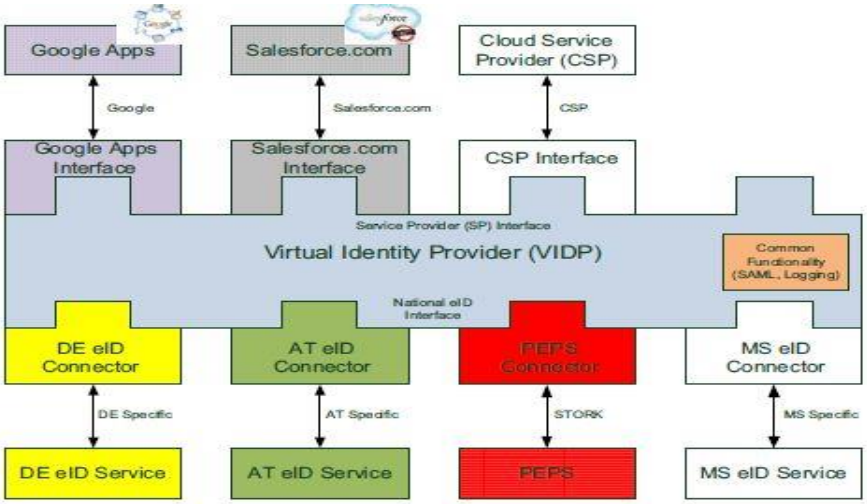

Fig. 2 Extended VIDP architecture supporting eID based cloud authentication

The structure of the proposed REMOGO comprises of data collection services, decision support system, an authentication centre, as well as a filtered database that is available and can be used by any other country where refugees are transferred. The flowchart in figure 3 shows the whole process with its various steps, where the system can decide if a refugee can justify the rights for asylum or to proceed for repatriation.

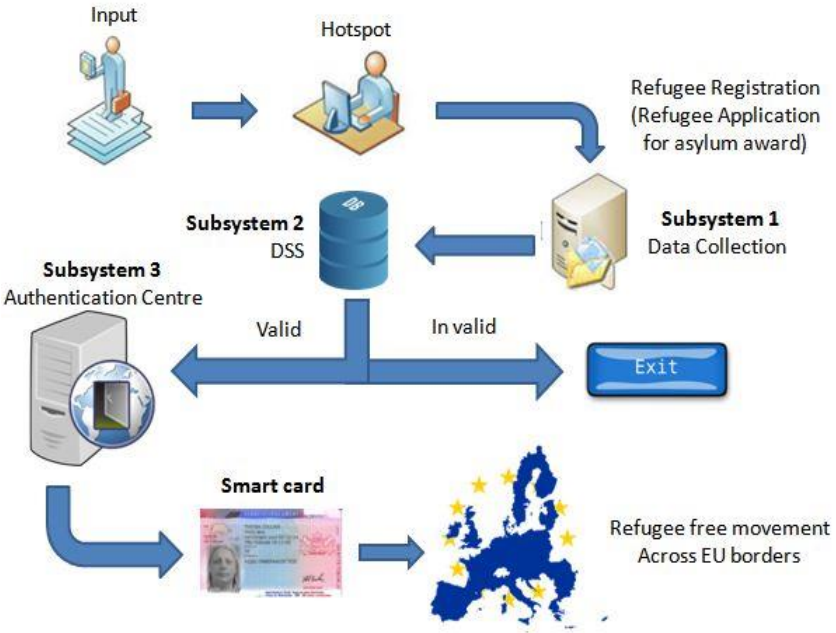

Fig. 3 Authentication Process in REMOGO system

3 eID procedure

The European Digital Agenda, the European Action Plan on e-Government (2011-2015) and the European Directive on Electronic Services, underlined the importance of a pan-European interoperability framework for Electronic Identification (eID) for e-Government services (Sideridis et al., 2015; European Interoperability Framework, 2014; European Commission, 2010c). The European Commission (EC) have launched, under the ICT Policy Support Programme (EUR-Lex a) of the Competitiveness and Innovation Framework Programme (CIP), several Large Scale Pilots (LSPs) on different policy domains in order to facilitate the goal of the Digital Single Market, among them: STORK1.0 (STORK 1.0a) & STORK2.0 (STORK 2.0c) (e-identification), PEPPOL (e-procurement) (PEPPOL), SPOCS (Spocs) (Points of Single Contact), epSOS (epSOS) (e-Health) and e-CODEX (e-CODEX) (e-justice). eSENS (e-SENS) is an another LSP that EC lunched on 2013 and is expected to be completed by the end of 2016. The main goal of eSENS is to combine the produced solutions from the previous LSPs in order to provide cross-border and cross–domain re-usable solutions for electronic services in public administration and facilitate easy access to public administration online.

The provided LSPs solutions are delivered as Building Blocks (BBs) which are in principal interoperability agreements (semantic and technical) along with a sample software implementation between the European Union member states that have participated in the LSPs. The EC's Connecting Europe Facilities Program (CEF) (European Commission e) ensures the sustainability of certain BBs by filling legal and technical gaps, retain them updated and offer them to EU countries ready to be combined and integrated with minimal adaptations to any domain electronic services at European, national or local level. On 31th of March 2016 CEF lunched the Digital Single Web Portal where all the needed information on the CEF's BBs can be found in an attempt to encourage MSs to extend their services with cross border functionalities.

One of the most needed BB for the provision of an electronic service in all domains is the eID BB. Citizens, Businesses (Natural or Legal Persons) and Public Servants need to authenticate themselves in order to be authorized and gain access to a protected resource by verifying in a secure, reliable and trusted way their identity and (or) their role (i.e. acting on behalf of a company or as a Layer). STORK1.0 provided the first eID BB while STORK2.0 extended it by demonstrating the capability of the provision of additional attributes by trusted Attribute Providers (AP).

While STORK1.0 & STORK2.0 offered the first eID BB solution along with a software reference implementation, the EC covered the needs on legal interoperability by introducing the EU Regulation No 910/2014 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 European Parliament and the Council of 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 is the mandatory cross-border recognition of the authentication schemes of all the MS 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. The four scaled STORK Quality Assurance Authentication (QAA) (EUR-Lex a) levels have been considered on the determination of the eIDAS LoA (Table 1). Every IDP shall make available, on request, the user's level of quality of the authentication in order to enable each Services Provider (SP) 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 taking into account also the STORK 1.0 & STORK 2.0 eID Interoperability Framework that has been established during the projects. The Framework is consisting of several national nodes acting as proxy servers (Pan-European Proxy Services -PEPS) or Middlewares (Middleware Solution MW- VIDP) depending on the architectural solution that has been followed by the MS country (STORK 1.0b; STORK 2.0c). 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 MS should be transparent to the other MSs.

Under the above regulation seven Implementation Decisions[1] have been issued at the time of writing, covering organizational and technical subjects. In parallel with the Implementation Decisions, the technical specifications for the eIDAS Interoperability Framework, a sample implementation of the eIDAS node (OASIS, 2008) and of a Digital Signature Service (STORK 1.0c) have also been published. These will assist Member States with the implementation of the Regulation. The eIDAS interoperability framework and the eIDAS node implementation are based on the STORK eID interoperability framework and nodes but there are some differences on the implementation rendering them incompatible. CEF program in collaboration with eSENS project are creating a software adapter in order to make feasible the interoperability between STORK2.0 and the eIDAS nodes. This adapter will be used by the STORK2.0 MS countries until they will upgrade their nodes with the eIDAS nodes.

The identification and authentication processes are based on message exchanging that include personal and technical attributes. STORK projects used a modified Kantara Initiative eGovernment Implementation Profile of SAML V2.0 (STORK 1.0, 2010; 2007) in order to exchange those messages. Under eIDAS technical specifications both SAML2.0 and STORK technical specifications has been encountered. SAML standard is based on the XML language providing the capability to exchange identity characteristics through the payload of the assertions SAML, as long as those characteristics can be represented in XML language. A SAML assertion is a package of security information encoded in XML and includes a number of elements about the issuer, the subject, attribute and authentication statements, conditions and other state-

[1] https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

ments. The main differences between KANTARA SAML V2.0 and STORK SAML 2.0 protocols are that STORK2.0 SAML includes information on the Authentication Requests: (a) about the LoA which represents the quality assurance Level of Authentication of the eID scheme, (b) supports additional STORK attributes,(c) include information regarding the allowance of cross border and cross sector sharing of an eID and (d) include information on the existence of any other additional attributes. Moreover, in STORK SAML protocol all the communications are by default and compulsorily digitally signed with an XML Signature. By digitally signing the requesting and receiving assertions the requestor or sender are being authenticated, ensuring the integrity of the exchanged assertions.

Figure 4 below demonstrates a STORK2.0 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 MS 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 C-PEPS (Citizen's PEPS) or as S-PEPS (Service 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 the identity attributes are needed and STORK2.0 support them, the user will be asked to choose the source of the attributes (AP), 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 service provider (1);
- The service provider 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 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.

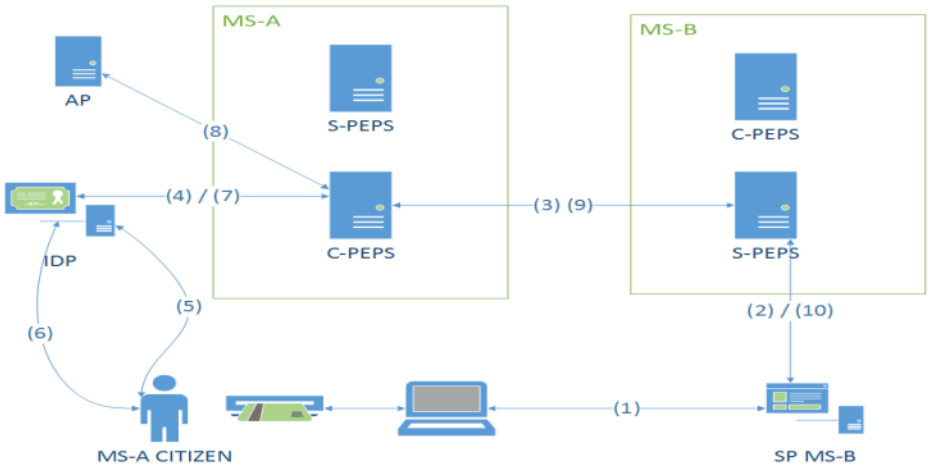

Fig. 4 Cross Border Authentication through STORK 2.0

In the case where eIDAS nodes are used instead of PEPS nodes, the procedure is the same. The only difference is that APs are not supported on the current version of the eIDAS node. Cross border authentication is expected to increase the effectiveness of public and private online services, e-business and electronic commerce in the EU.

4 Refugee Mobility Smart Cross Boarder System

The proposal in this paper for the development of a prototype of the **Re**fugee **Mo**bility Smart Cross Border e-**Go**vernment– (**ReMoGo**) system, as an enhanced application of SCBeG systems modeling, fully described in (Sideridis and Stamelos, 1988), will add maximum value and impact if the European Commission were to adopt it and proceed with the appropriate steps for its implementation. Of course, ReMoGo must be considered as part of a **complete refugee installation and mobility response plan** to a problem which inherently requires urgent attention. To some readers this recommendation may sound as a luxury when compared to the huge social issue of the refugee crisis in a worldwide scale. Information from Syrian colleagues and postgraduate students researching abroad confirm that life is still going on in the country and governmental organizations, at least those operating in no-war zones, continue to work and serve as normally as possible. Furthermore, one of the authors has had first-hand experience of a similarly desperate situation where their project proposal met with a very successful implementation and excellent results. At the time the crisis facing the authorities and requiring an immediate response was that of thousands of earthquake victims in the city of Kalamata in Southern Greece. Registration, verification and establishment of status and compensation categories were the

key requirements at the time (BBC, 2016a). A full utilization of the available, at that time, ICT tools had effectively helped to minimize bureaucratic and other problems hindering the main task of a complete Governmental response plan to a tremendous social problem itself.

Before any steps are to be taken, the refugee's mobility problem has to be clearly described in order to successfully address its requirements. The application of appropriate tools and advanced techniques, described briefly in previous sections of this paper, is necessary so that the proposed solution will be efficient, secure and reliable. The development of the SCBeG model itself will follow the steps described in (Sideridis and Stamelos, 1988) whereas the complete project will follow the well-known four steps of the Project Management Theory. These steps are described below in short, for reasons of completion. They are: (i). **Project Conception, Definition and Planning**. This is a very important step since it provides reasons for adopting or not the project proposal and actually implementing the project in full. Because of its great importance it may be found in the literature split in two steps (Project Conception and Project Definition and Planning). This step includes the study area with regard refugee's legal status and their eligibility of mobility in various countries in accordance with the European Commission's Directive (ICAO, 2015), the Common European Asylum System / *Home Affairs* and the implementation of the 1951 Geneva Convention relating to the Status of Refugees, their rights and the legal obligations of States. It also examines if the system proposed will be of real benefit to supporting organisations. At this point, a decision should be made on a realistic examination of all the parameters of the problem under consideration and of the selection of the appropriate team involved for its implementation. During this step, the project also will be analytically described in writing. Charters and detailed flows to be followed should be given. Timetables, personnel involved, resources, budget and priorities should also clearly defined. (ii) **Project Launch**. This step should follow a positive decision made by the organisation(s) involved taking into account the presumptions of the previous step. Now is the correct time for a distribution of tasks and responsibilities to the personnel involved. (iii) **Project Performance and Control**. By now the project management team will be in a position to compare the progress made according to schedule and the actual plan. A readjustment of schedules may be necessary and finally step (iv) **Project Close and Evaluation**. The successful implementation of all project's tasks is followed by the project evaluation by the organisation in charge. Following the theory above, we shortly outline below step 1 of the proposed project for the development of the ReMoGo system.

4.1 ReMoGo Conception, Definition and Planning

The European Union (EU) Member States follow a Common European Asylum (issuing) System (CEAS) fully described in Directive X3 shown in figure 5 below. In particular according to article 8 of this Directive:

The European Council at its meeting of 10-11/2/2009 adopted the Stockholm Programme which reiterated the commitment to the objective of establishing by 2012 a common era of protection and solidarity based on a common asylum procedure and a

uniform status for those granted international protection standards and fair and effective procedures. Also, the Stockholm Programme affirmed that "...people in need of international protection should be offered the same level of treatment as regard procedural arrangements and status determination regardless of the Member State in which their application for international protection is lodged. Similar cases should be treated alike".

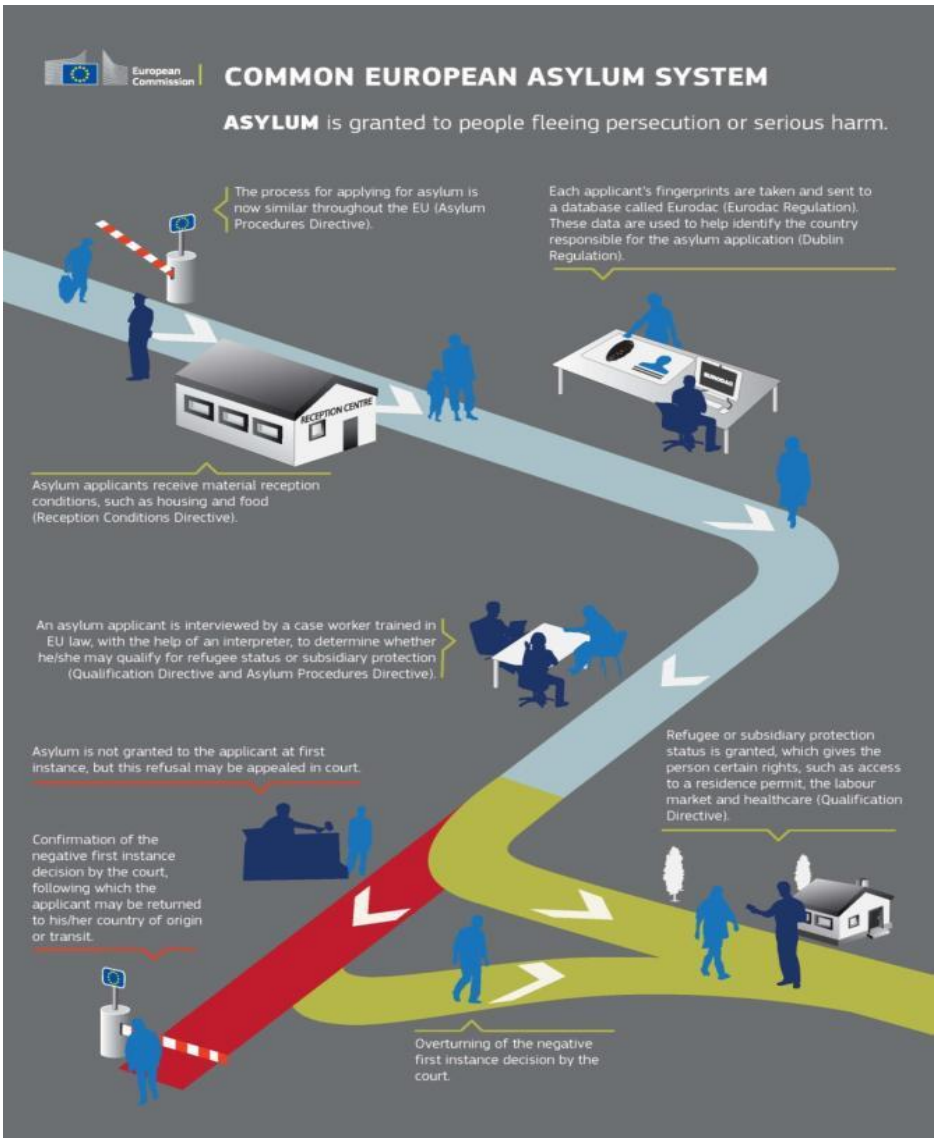

Fig. 5 Common European Asylum System

The application of the CEAS is analytically and procedurally presented in a laboriously written EU paper of the EU Home Affairs (European Union b). This doc-

ument is of great value for the actual implementation of the ReMoGo system subject, of course, to certain more recent developments in the present refugee crisis situation. These recent developments dictate regulations resulting from the Heads of State or Government agreements, during the EU Heads of State or Government Summits of March the 7th and 18th, 2016, in Brussels (European Council a). The regulations are considering legal and/or illegal refugees mobility and through the recently established Emergency Response Coordination Centre (ERCC) provide prerequisites which must be added to those of CEAS before any steps will be taken for its implementation. The ERCC is publishing daily maps (Emergency Response Coordination Centre, 2016) showing the actual movements of refugees (legal or not) during this peak period of the refugee crisis problem.

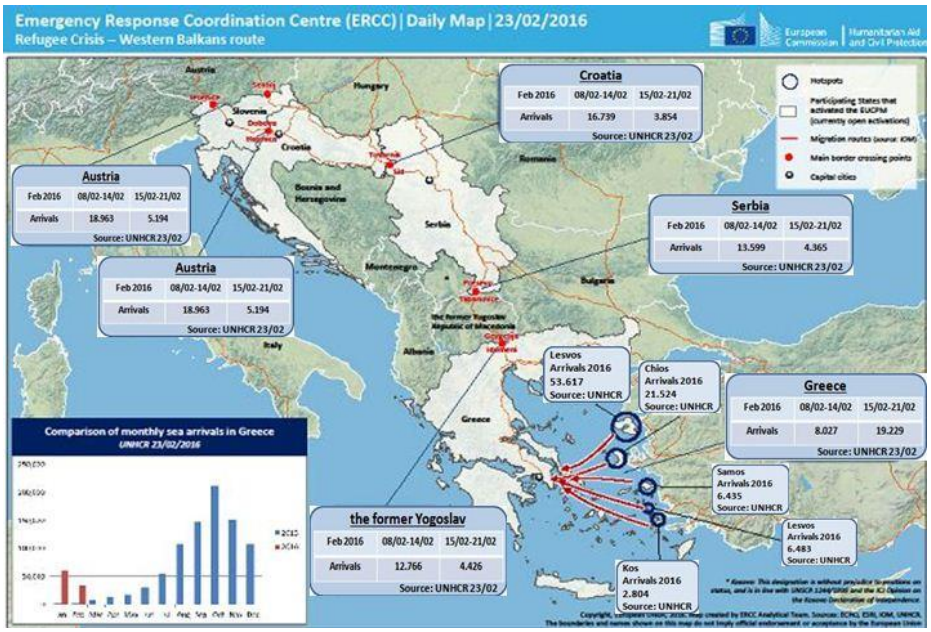

Fig. 6 EU's Emergency Response Coordination Centre: daily map of 23/02/2016

The proposed ReMoGo system includes three subsystems. A brief description of each of the three subsystems is given below and they are pictorially presented in the flow chart shown in figure 7. Taking into account the existing refugee's data and any new details emerging from an interview in connection with the conditions for asylum award (Subsystem A), the system proceeds to the assessment of the application and the appropriate decision (Subsystem B). In case of a negative decision from the Official Committee in charge, the system notifies the applicant accordingly providing also its reasoning and official information regarding its right to appeal to the Ministry of Justice of the country involved. In case of a positive decision to the applicant's appeal, the system: (i) notifies the applicant for its right to residence permit (ii) proceeds to complete and verify applicant's data in the data collection module of Subsystem A and (iii) issues an electronic card compatible with the International

Civil Aviation Organization (ICAO) standards (Commission Of The European Communities, 2003).

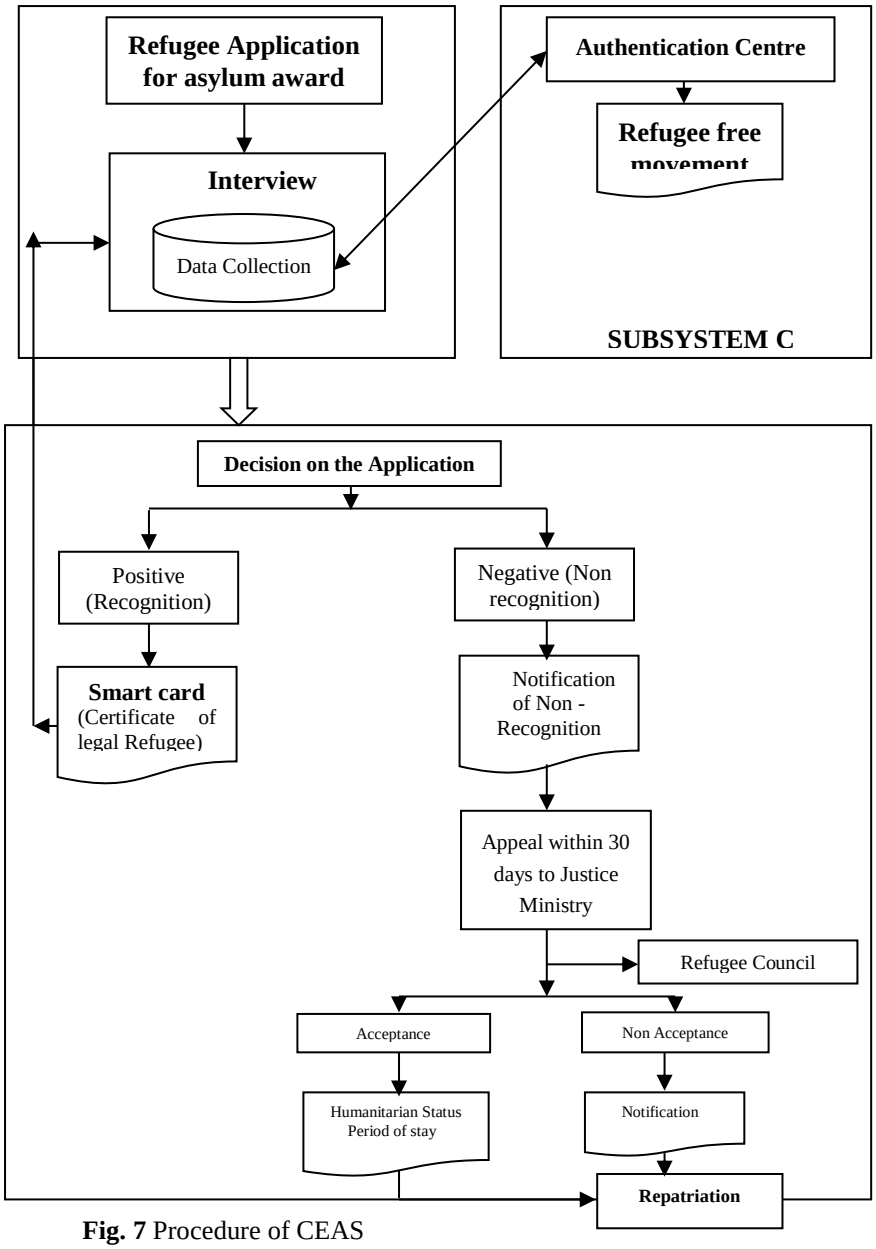

Fig. 7 Procedure of CEAS

The database of subsystem A collates and stores data gathered during the data collection phase of the process. An applicant's data stored in this database are sent to the Authentication Centre (AuCe) and they are authenticated at any point at which the refugee wishes to move into an EU State or any other country allowed in accordance to the decision in response to this refugee's initial application.
The authors propose to integrate the Authentication Centre with the eID Interoperability Framework that has been established by the EC in the context of the eIDAS regulation (fig. 8). Bureaucrats designing the legislative and authoritative system of implementing EU's and national governments' decisions are questioning themselves of how are they are going to manually authenticate and check such data with authorities of countries facing a war state and not having the appropriate data exchange agreements with EU. The proposed REMOGO system will adopt any form of decision they are bound to make and import it to the system which is designed to alleviate bureaucracy to any step of the complete process that can be automated. The tantalizing questions as to the lack of data exchange infrastructure in war torn countries such as Syria and Afghanistan can be alleviated by the fact that these countries still exist and function. Their services might be affected but still partially run as before and will give first priority in providing adequate answers to all questions of this kind. The AuCe could act as an IDP of the refugees by filling all the requirements of the regulation in order to provide electronic authentication equal to "high" Level of Authentication (LoA). The AuCe could be integrated and combined with the Eurodac and VIS systems in order to ensure the unique identification of the eID holders that are registered at the Registration Centre. Refugees should be provided with eIDs and will be empowered to use them in order to access government services in any European Country that they will settle or travel within. It is recognized that there are a lot of burdens and difficulties at the registration phase as in many cases in the countries of origin of the refugees the government structure is not operational due to war. This will add complexity during the registration as in many cases it will not be feasible to verify the quality and the validity of the provided registration information. Artificial Intelligence Algorithms and Decision Support Information Systems could be used in supporting the proposed system in order to detect high risk cases for incompatibility or anomalies in the registration data. These systems can take into account statistical geoinformation regarding the existence and the occurrences of the declared names in certain areas or the spoken language etc. The systems could also help the interviewers to confirm the declared country of origin of the asylum-seekers.

Once a refugee has been issued with an electronic identification card she/he could use it in any EU country in order to access Government Services. The flow of the electronic identification procedure is the same with the one that described in Section 2. Visa Information System (VIS), Schengen Information System (SIS), Passenger Name Record (PNR) could act as APs and inform the SPs of any changes on the status of the legality of the eID user.

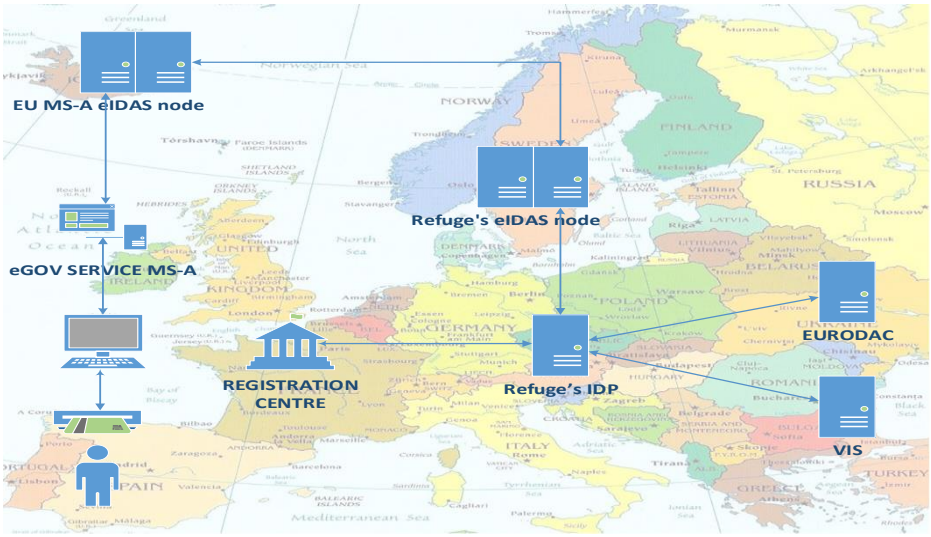

Fig. 8 EIDAS regulation

5 Discussion

E-government systems, procedures and their integration with the more recent electronic identification systems comprise a major breakthrough in electronic services provision and integration across the European Union. In particular the outcomes of the Stock 2.0 project have demonstrated the strength and readiness of such systems. Beyond the pilot schemes that these systems have been tested the uptake is still slow and certainly has not paid back the huge expenses that the EU has contributed towards research and development. However sinister this may sound, the current refugee crisis is an excellent opportunity to demonstrate the benefits of such systems.

E-government systems and services have often been criticized as to the rather low contribution to enhanced efficiency in service provision they have delivered in certain service sectors (Pimenidis and Georgiadis, 2014; Pimenidis et al., 2011). In the present situation the need to improve the way the processing and subsequent transport management of refugee's is conducted is critical. Despite efforts to stem the flow and the creation of refugee camps, at present there are very large numbers of people expecting to be processed, progressed and transported that have been left in doubt and agony (BBC, 2016a; BBC, 2016b). The main reason for the stranding of these people is the lack of coordination and the lack of a common system for processing the individual information of such persons. Under these conditions refugees are processed slowly, risk health and are exposed to other malicious risks due to their mass concentration under difficult conditions. Furthermore the refugees themselves could develop into a social threat to local societies (The Guardian, 2016). The various organizations that are involved in processing and supporting these stranded people, often due to lack of coordination and proper sharing pf information, accuse each other of errors and

there is always the risk of the wrong people (ones that could be under severe risk) returned to their home countries while at the same time people that could be dangerous to the receiving countries are granted asylum and free entry with potentially grave results of terrorist activities.

The system proposed here is simple in its implementation, can operate under makeshift conditions in camps and other areas where refugees are housed temporarily and can offer secure and verified means of processing their application and personal data efficiently. The results can be obtained, in an orderly and efficient way and in a secure environment (Papadopoulou et al., 2015). The probability of error is minimal and the accuracy of the decisions will be very high as these systems have been tested extensively. Thus the process of further transporting the people at the center of the crisis to desired destinations or back to their countries of origin will be performed in a much more effective way, faster and without any doubts as to the accuracy and the justification of the decisions behind the moves (Athanasopoulos et al., 2015).

The success of such a system will not be limited to the present refugee crisis. Even if the world were to develop into a peaceful place and no more wars were to be fought in the future, it is highly unlikely that there would be no natural disasters. These often create victims and people in need which is far more urgent than the processing of people that might be stranded in a place that is not necessarily comfortable but at least is safe. The need for efficiency and effectiveness in responding to such crisis situations would prove the proposed system ideal. The previous experience of running a similar system under makeshift conditions and with much less reliable infrastructure demonstrates the dynamics of such systems to make use of mobile networks and Wi-Fi systems to support the necessary communications even under severe conditions (Sideridis and Stamelos 1988). As to the latter, various applications of online services in the developing world have demonstrated in the recent past that a mobile network can prove a suitable and effective medium of communication and support infrastructure (Pimenidis et al., 2009).

Given the urgency of the situation, the previous experience and the state of the art technologies available from the recent research outputs and extensive pilot studies by EU research and work teams; the authors believe that their proposal is both viable and possibly the only realistic solution in supporting and effectively resolving all the technical issues pertaining the processing and efficient management of the present refugee crisis in Europe. The implementation and use of the proposed ReMoGo system will open the road for the development of similar systems that could support the collaboration across states in different regions around the globe. The efficient processing of data in each case and the accuracy of information provided will effectively support aid efforts in addressing the aftermath of natural disasters, epidemics and even future refugee crisis, in the developed and the developing world alike.

6 Conclusions

The recent refugee crisis in Europe demands a secure and innovative way of handling data and information effectively and efficiently to allow the various authorities across the continent to register the large numbers of seeking refugee asylum. Recently completed work on extensively validated cross border identification systems

across the European Union can be combined with existing experience of handling data under extreme conditions in addressing emergency situations on a large scale.

The proposed Refugee Mobility Smart Cross Border e-Government (ReMoGo) system is an integration of cross border identification systems with local large scale data management systems. The authors believe that such implementation can establish a new era in the way large scale crises are handled across the globe. Such systems will continue to evolve as research and technology progress, but are at present ready to deliver effective solutions.

References

Analytical Team of Emergency Response Coordination Centre (ERCC), Daily Map of 23/02/2016 [online] http://reliefweb.int/sites/reliefweb.int/files/resources/ECDM_20160223_WesternBalkans.pdf/ (Accessed 23/04/2016).

Athanasopoulos, E, Boehner, M, Ioannidis, S, Giuffrida, C, Pidan, D, Prevelakis, V, and Ioannis Sourdis, I, Strydis, C, and Thomson, J. (2015) 'Secure Hardware-Software Architectures for Robust Computing Systems', S.K. Katsikas and A.B. Sideridis (Eds.): E-Democracy 2015, CCIS 570, pp. 209–212.

BBC 2016a. [online] http://www.bbc.co.uk/news/world-europe-34131911/ (accessed 02/05/2016).

BBC 2016b. [online] http://www.bbc.co.uk/news/world-europe-36054840/ (accessed 02/05/2016).

CEF building blocks. [online] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+building+blocks/ (Accessed 21/04/2016).

E-Justice Communication via Online Data Exchange, e-CODEX. [online] http://www.e-codex.eu/home.html (Accessed 20/04/2016).

EUR-Lex (a), Decision No 1639/2006/EC of the European Parliament and of the Council of 24 October 2006 establishing a Competitiveness and Innovation Framework Programme (2007 to 2013) — OJ L 310, 09.11.2006, p. 15. 11 COM (2009) 247. [online] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006D1639/ (Accessed 19/04/2016).

Electronic Simple European Networked Services, eSENS. [online] https://www.esens.eu/ (Accessed 20/04/2016).

Euractiv (a). [online] http://www.euractiv.com/section/digital/news/2020-plan-pins-hopes-on-digital-agenda/ (Accessed 14/04/2016).

Euractiv (b). [online] http://www.euractiv.com/section/justice-home-affairs/news/eurodac-fingerprint-database-under-fire-by-human-rights-activists/ (Accessed 18/04/2016).

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).

European Commission (a). [online] http://ec.europa.eu/information_society/apps/projects/ (Accessed 23/04/2016).

European Commission (b). [online] http://ec.europa.eu/digital-agenda/en/connecting-euro pe-facility/ (Accessed 17/04/2016).

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).

European Commission (d). [online] http://ec.europa.eu/isa/ (Accessed 17/04/2016).

European Commission (e), Linking up Europe: the Importance of Interoperability for eGovernment Service. [online] http://ec.europa.eu/idabc/servlets/Doc2bb8.pdf?id=1675/ (accessed 15/04/2016).

European Commission, 2016a. [online] http://ec.europa.eu/digital-agenda/en/digital-agenda-europe-2020-strategy/ (Accessed 17/04/2016).

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).

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).

European Commission, 2010c. [online] http://ec.europa.eu/digital-agenda/en/ict-policy-support-programme/ (Accessed 23/04/2016).

European Interoperability Framework For Pan-European eGovernment Services, 2004: Belgium. [online] http://ec.europa.eu/idabc/servlets/Docd552.pdf?id=19529/ (Accessed 19/04/2016).

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.

European Patients - Smart open Services, epSOS, [online] http://www.epsos.eu/ (Accessed 20/04/2016).

European Union (b), A Common European Asylum System, Luxembourg: Publication Office, ISBN 978-92-79-34626-2.

International Civil Aviation Organization (ICAO), (2015) Document 9303: Machine Readable Travel Documents, 7th edition. [online] http://www.icao.int/publications/pages /publication.aspx?docnum=9303/ (Accessed 20/04/2016).

Leitold H., (2009) 'STORK Overview'. [online] https://online.tugraz.at/tug_online/ voe_ main2.getvolltext?pCurrPk=44744 (Accessed 17/04/2016).

Nielsen S., (2001) 'A Simple Model of Commodity Taxation and Cross-border Shopping', Scand J. of Economics.

Pan-European Public Procurement Online, PEPPOL. [online] https://www.peppol.eu/ (Accessed 20/04/2016).

Papadopoulou M-E, Ch., Patrikakis, C.Z.,Venieris, I.S. and Kaklamani, D-T, I. (2015) 'On the Use of a Secure and Privacy-Aware eGovernment Infrastructure: The SPAGOS Framework', S.K. Katsikas and A.B. Sideridis (Eds.): E-Democracy 2015, CCIS 570, pp. 223–227.

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, January-March 2014.

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.

Pimenidis E, Sideridis A.B, Antonopoulou E (2009) 'Mobile Devices and Services: Bridging the Digital Divide in Rural Areas', International Journal of Electronic Security and Digital Forensics (IJESDF), Vol. 2, No. 4, pp. 424-434.

Security Assertion Markup Language (SAML) V2.0 Technical Overview. [online] https:// www.oasis-open.org/committees/download.php/20645/sstc-saml-tech-overview-2%200-draft-10.pdf/ (Accessed 22/04/2016).

Sideridis A. B., (2013), 'Present and future e-Government advances at the service of rural area citizens', Proceedings, Agricultural Informatics 2013: The past, the present and future of Agricultural Informatics. International Conference, 8-9. November, 2013, Debrecen, Hungary.

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.

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.

Sideridis A. B. and Stamelos D., (1988) Data Processing for earthquake victims in Greece, Information and Management Vol. 15, pp. 255-260.

Simple Procedures Online for Cross - Border Services, SPOCS. [online] http://www.eu-spocs.eu/ (Accessed 20/04/2016).

STORK 1.0 (a). [online] https://www.eid-stork.eu/ (Accessed 20/04/2016).

STORK 1.0 (b) eID Consortium, D2.3 Quality authenticator schem. [online] http://www.eid-stork.eu/ (Accessed 22/04/2016).

STORK 1.0 (c) eID Consortium, D 3.2.1 SAML. [online] http://www.eid-stork.eu/ (Accessed 22/04/2016).

STORK 2.0 (a). [online] https://www.eid-stork2.eu/ (Accessed 12/04/2016).

STORK 2.0. (b), [online] https://www.eid-stork2.eu/images/stories/documents/ETSI%20 2015%20presentation% 20-STORK%202.0.pdf/ (Accessed 14/04/2016).

STORK 2.0 (c). [online] https://www.eid-stork2.eu/ (Accessed 20/04/2016).

STORK 2.0 (d) eID Consortium, D4.3 First Version of Technical Design. [online] https://www.eidstork2.eu/ (Accessed 22/04/2016).

Tauber A. et al, (2012) 'Approaching the challenge of eID Interoperability: An Austrian Perspective', European Journal of ePractice, no 14.

The Guardian, EU relocates just 208 refugees from Greece after deal with Turkey [online] http://www.theguardian.com/world/2016/apr/15/eu-relocates-just-208-refugees-from-greece-after-deal-with-turkey/ (accessed 15/04/2016).