

Implementation Issues of Cross Border e-Government Systems and Services

Loucas Protopappas¹, Alexander. B. Sideridis², Costas P. Yialouris²

¹Informatics Laboratory, Agricultural University of Athens, 75, Iera Odos str., Athens 118 55, Greece; e-mail: loucas.protopappas@gmail.com

²Informatics Laboratory, Agricultural University of Athens, 75, Iera Odos str., Athens 118 55, Greece; e-mail: as@aau.gr

³Informatics Laboratory, Agricultural University of Athens, 75, Iera Odos str., Athens 118 55, Greece; e-mail: yialouris@aau.gr

Abstract. Within the context of the European Union member states cross-collaboration for the delivery of seamless e-Government systems, the cross-border strategies have flourished during the last few years across Europe. Specifically, worldwide various innovative programs have been implemented and a considerable number of initiatives took place for upgrading these systems or announcing new ones mostly based on advances on Artificial Intelligence. In addition, the integration of new emerging technologies (Cloud Computing, Big Data and Internet of Things) into existing or designing new systems and services, combined with the use of readymade platforms in Europe of e-Authentication, e-Signature and e-Identification opened up a new perspective on cross-border e-government for security-sensitive areas such as Life Sciences (e-Health, e-Banking, e-Immigration, Smart Agriculture, e-Food etc). Meanwhile, the variety and complexity of e-government initiatives implies the existence of a wide range of challenges and barriers to its implementation and management. This paper mainly focuses on identifying and overcoming the implementation challenges of cross-border e-government systems as European governments must make efforts to fill in the gaps and barriers across several categories, including organizational, semantic, technical, policy and regulation issues, such as lack of government integration, privacy, heterogeneous national systems and lack of shared standards and compatible infrastructure among EU countries.

Keywords: e-Government systems; Implementation issues; Authentication; Electronic Identification; Cloud Computing.

1 Introduction

In the light of the required cross-border mobility, the level of maturity of e-Gov services, provided by the Member States of the European Union has increased significantly, gaining more and more of the trust of citizens and businesses. Existing government e-services are an important part for the development of many sectors, such as of economy, employment, agriculture, health, at national and cross-border

Copyright © 2020 for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

Proceedings of the 9th International Conference on Information and Communication Technologies in Agriculture, Food & Environment (HAICTA 2020), Thessaloniki, Greece, September 24-27, 2020.

level [1]. According to recently published reports, they also increase the innovation index, create new services for businesses, contribute to budget savings, increase public revenues and ultimately create the conditions for the development of new business activities and jobs [2].

The perspectives of promising cross-border cooperation between EU Member States can create many challenges, which have already been designed at operational, semantic and technical level by the European Union. However, the driving forces are the innovative European Programs (Interreg, One-Stop-Government and “Once-Only” Principle Projects (TOOP)) [3][5], which carried out actions of cross-border cooperation and laid the foundations for further development of the existing government systems. For the last 5 years, at European level, there has been a hodgepodge of actions and programs, all of which tried to provide integrated e-government systems, but the provision of such systems remains fragmented. It is clear that borders are a complex multidimensional phenomenon in Europe as there are many dimensions that need to be addressed (political, economic, legal, technical, linguistic and cultural) in order for the cross-border cooperation to deliver results [4] [6].

The need for secure and reliable e-services is a key objective for the European Union and the governments of the Member States which to a large extent were treated primarily as national affairs. However, e-government services are in a dynamic process of Europeanization and very careful steps must be taken to remove chronic vulnerabilities within existing systems of Life Sciences (e-health, e-justice, e-banking, e-migration, e-agriculture, etc.) at a cross-border level [7].

Certainly, now the ready-made software platforms e-Authentication (e-AU), e-SIGNatures (e-SIGN) and e-Identification (e-ID) and, in conjunction with emerging technologies (Cloud Computing, Big Data and Internet of Things) shape the roadmap for transforming existing services into smart cross-border ones, offering increased security, standardization and interoperability. Along with these perspectives, the proposed smart cross-border government systems (SCBeG) that incorporate innovative technological features to be utilised in order to solve some of the issues which are mentioned below [6].

It is clear that for transforming the national government agencies in order to function reliably and fully functionally at the cross-border level, important parameters of each system must be considered, as each member state of the European Union has its own peculiarities and unique characteristics. A representative example is the health sector as it is considered to be one of the most data sensitive sectors as health professionals continue to face different (potential) obstacles due to dissimilarities of rules between MSs, various (cross-sectorial) administrative requirements and unspecified secure way of delivering patients' personal data [7][8].

This paper attempts to clarify the obstacles and technical difficulties that may arise from transforming national systems of government into a cross-border environment. Section 2 presents current developments in cross-border systems. Section 3 presents the obstacles and vulnerabilities in the integration of systems. Finally, in the fourth section draws conclusions from the adoption at the level of productive use of cross border systems.

2 Current Developments in cross-border systems

Nowadays, cross-border e-government services are booming, and this is due to many reasons. First, the need to transform national government systems was imperative as the world trade is flourishing rapidly, the movement of citizens within European borders is continuous and the central government of each Member State was Europeanized, acting as a cross-border bridge. It is obvious that the European citizen should be able to use any e-government service of his country, wherever he is, for instance, his medical history, his criminal record, even for a document from the registry office of his city [9].

Secondly, the contribution of cross-border cooperation between EU Member States, known as Interreg A, launches a European territorial cooperation, which is divided into internal and external border cooperation [10]. This European model divides Member States into structures, which usually consist of public authorities (municipalities, regions, counties, regions) from different countries, organized into working communities, European regions or EGTCs (European Grouping of Territorial Cooperation) [11].

European programs running at the moment significantly promote maturation and upgrading of existing cross-governmental systems, while laying the foundations for new smart cross border systems that will fit perfectly into European standards and will face obstacles to necessary and imminent transformation of national government systems [12].

The European Commission has taken concrete actions to develop cross-border digital public services and, through integrated and customer-oriented mechanisms (One-stop Government and Once-Only Principle Project (TOOP)) [5], aims to implement automated, secure and reliable e-government services. Citizens and especially businesses can benefit significantly from the implementation of the aforementioned projects as they will be able to complete their legal obligations with reduced administrative burden, time savings and cost minimization. At the same time, the data that will be handled during the transactions of the public administrations will always remain under the protection and the consent of the companies involved, applying with the EU data protection legislation [13].

Clearly, the contribution of European actions is crucial as they define the models that encourage the design of sophisticated e-government systems to address technical and organizational problems, and in particular the secure exchange of personal or confidential information. However, from a technical point of view, the integrated European projects have left behind important tools, which can ensure the required security, interoperability and seamless operation of cross-border systems. The ready-made platforms of e-AUthentication (e-AU), e-SIGNature (e-SIGN) and e-IDentification (e-ID), which are deliverable of the pan-European STORK 2.0 project, created a single Electronic Identification and Authentication area for Europe. Expecting this foreseeable development, ongoing European eGovernment projects are based on experience and previous work from relevant projects (eg STORK, STORK 2.0, e-SENS, e-CODEX and PEPPOL) in order to fill the existing gaps and obstacles, for which this document aims to propose solutions [14] – [18].

However, in order for a natural or legal person of a particular state to be able to enjoy the E-Gov services offered by another EU state, the administrations and their respective information systems must have the appropriate technical infrastructure to interact with each other. The following figure shows the interactions required to enable a cross-border transaction between the public administrations of two Member States [19].

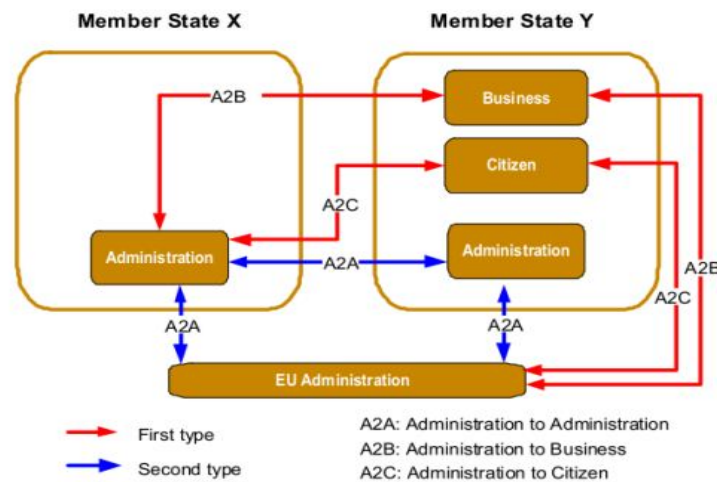


Fig 1. Transactions for the provision of public e-services at the cross-border level.

The first type illustrates the process required for the direct interaction between the businesses and citizens of one state with the public administrations of the other state (Administration-to-Business (A2B) and Administration-to-Citizen (A2C)) and the second concerns the process between the public administrations of the states involved but with the central administration of the EU (Administration-to-Administration (A2A)) [20].

Now, milestone in the functioning of cross-border government systems is eIDAS (electronic IDentification, Authentication and trust Services) regulation, which entered into force on 17 September 2014 and is effective from 1 July 2016 except some of its specific provisions contained in Article 52. All organizations providing digital services in an EU Member State must recognize electronic identification by all other EU Member States from 29 September 2018. The purpose of eIDAS is to monitor electronic authentication and trust services for electronic transactions within the EU Single Market. It regulates digital signatures, electronic transactions, the authorities involved, but also the integrated procedures to provide a secure way for users to manage their affairs online such as electronic funds transfer or transactions with public services [21][22].

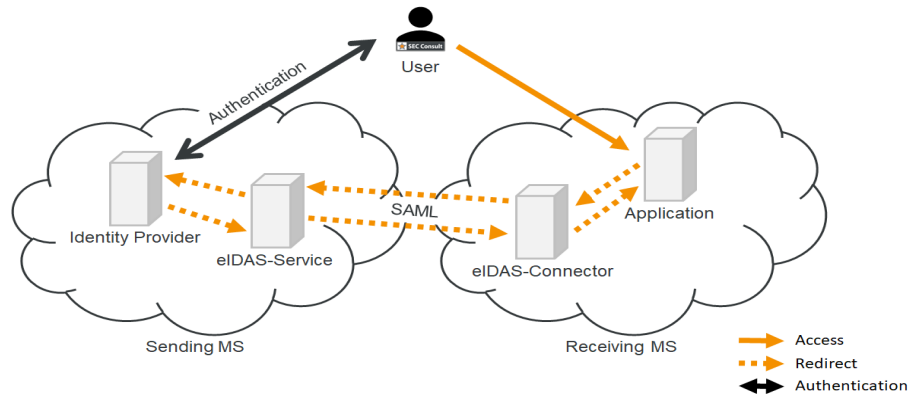


Fig 2. Schematic sequence of an authentication

Greece has fully implemented the eIDAS regulation, which has been incorporated in the majority of its public administrations and organizations. As recently announced by the President of the Athens Stock Exchange, the organization has managed to deal with bureaucratic issues, while at the same time, as a provider of Electronic Signature Certification Services, it is evaluated every year according to the WebTrust for Certification Authorities standard [31]. The other banking and academic organizations are moving in the same direction, as the former, through the eIDAS regulation, have benefited significantly, offering their customers increased security, greater data accuracy, less time-consuming procedures and a larger customer base while the latter use EIDAS node to ensure the connection of the Erasmus Exchange Student Identification Service (i.e. student mobility service) [32].

For the effective handling of complex cases in areas demanding global security for cross-border applications, in conjunction with the provided e-ID Interoperability Framework, which consists of several national nodes acting as pan-European proxy server services (PEPS) or intermediate devices (MW solution)), the use of emerging technologies Cloud Computing (CC), Internet of Things (IoT) and Big Data (BD) will offer unique features to existing cross-border systems. Therefore, the proposed Smart Cross Border e-Government (SCBeG) systems, making full use of ICT innovations and able to meet the requirements of the ever-changing and highly demanding cross-border environment [23] - [25].

However, there are similar European initiatives in the field of agriculture, as efforts are made to remove barriers to agricultural trade between countries to increase economic growth and access to safe, nutritious food at the cross-border level. Indicatively, a recent pilot project, AGROPOL, launched by the EC, provides practical guidance to strengthen agricultural production and the food industry through cross-border cooperation [34]. In the field of agriculture, the eIDAS regulation enables farmers, through their eID, to register areas across the border in the system of foreign agricultural services. This perspective will allow them to comply with EU law as, on the one hand, the animals do not cross the national borders, especially in mountain pastures and on the other hand in cases of declaration

of mountainous, unregistered areas. An example is the German-Dutch and Dutch-Belgian borders [34]. In addition, current technological advances, using the eIDAS approach, could also help farmers by providing secure transactions on foreign agricultural public agency portals, in order to apply for subsidy or registration of cattle.

More specifically, the steps that a farmer has to take from state A to state B are shown in the figure 3. The farmer, from state A, uses the eIDAS credentials, which were issued to him to connect the web portal (1). The system redirects the farmer to his national eIDAS node, where the required identification is performed (2) (3). Finally, the system when identifies the farmer provides him access to the provided electronic services (4) (5) [24].

Today, farmers and small and medium-sized agricultural enterprises, using smart government systems have decisive benefits, have the ability to further minimize bureaucracy, costs and time required in normal transactions. In addition, with the emerging technologies (IoT, AI, RFID, GPS and CC), farmers can automate a variety of processes, which until recently were laborious and required its physical presence in the field [35]. Thus, processes such as soil and plant monitoring, environmental monitoring and control systems and monitoring of important farm data (soil component, soil moisture, light, wind and air) are now available from any portable device. Therefore, galloping technology will significantly benefit the agricultural production sectors, providing increased profitability, sustainability and food safety and improving input efficiency [1].

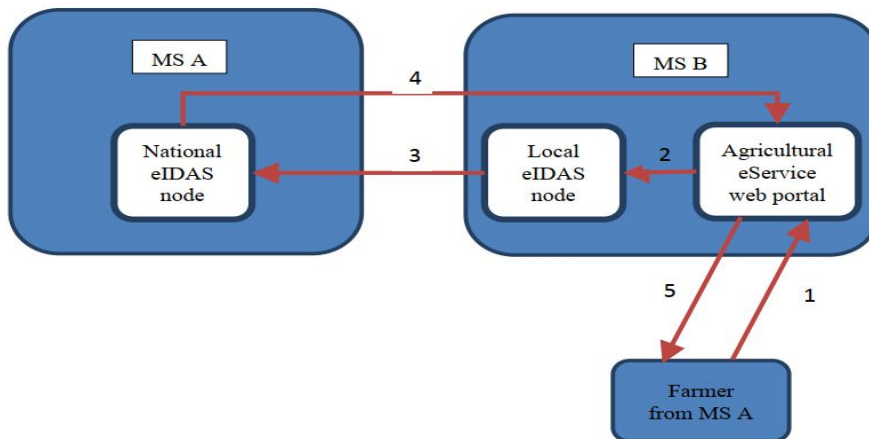


Fig 3. Agricultural e-service Web Portal Authentication Process

3 Barriers to the implementation of Cross-border E-Gov Systems

According to the European Interoperability Strategy (EIS) and other responsible organizations working to provide reliable and uninterrupted cross-border government services, interoperability is mentioned as one of the key aspects. However, equally important parameters, such as accessibility, security and protection of personal data, imply a wide range of challenges and obstacles in their implementation and management. The following figure shows the relations between the initiatives of the European Interoperability Framework [25] [26].

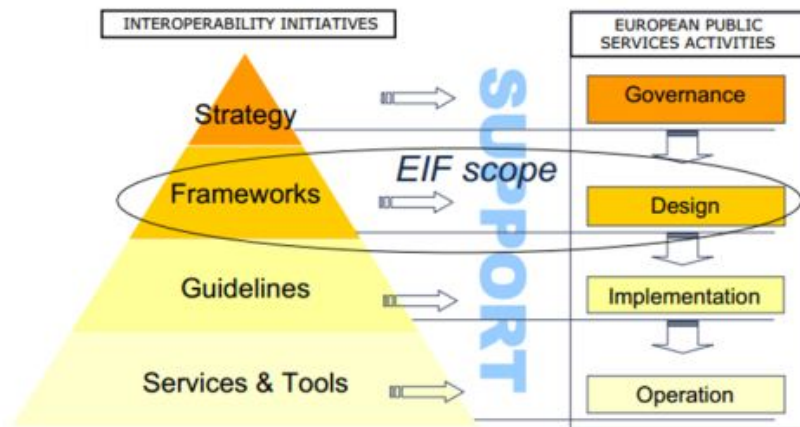


Fig 4. Interoperability initiatives to establish European cross-border public services

3.1 Accessibility

Ensuring equal opportunities for all through open, inclusive e-government systems is crucial to making them accessible to the public without discrimination. Interface design must follow some generally accepted principles in order to ensure access for people with disabilities and to offer support in a language that is understandable to the user. The Web Accessibility Guidelines set up by the World Wide Web Consortium of the Web Access Initiative must be followed [17].

3.2 Multilingualism

A wide variety of languages is used in the services offered in Europe. At the presentation level (front office and Internet sites - the level at which citizens and businesses interact with administrations), language is clearly an important factor in the effective implementation of cross-border e-Government services.

At the back-office level, the basic architectures should be linguistically neutral, so that multilingualism does not become an obstacle to the provision of HD services. If neutrality is not possible (eg in XML-systems), provisions should be made to facilitate translation mechanisms. Three common mechanisms that can address the issue of multilingualism are: a. separated instances for each language, b. shared content with a dynamic language switching and c. machine translations.

However, in the field of machine translations, with the help of artificial intelligence and Cloud Computing, a cross-border government service will be able to directly multi-language, based on neural network-based AI translation, interacting with the user, using innovative techniques such as Conversational User Interface (CUI), Machine Learning (ML) and Natural Language Processing (NLP) [30].

3.3 Security

Reliable exchange of information is carried out in accordance with established security policy. This is achieved by carrying out appropriate risk assessment actions, before the final definition and implementation of services and appropriate security measures. This principle also applies to cross-border services.

In this case, EU Member States will have to consider their own security policy and reach agreements to define a common security policy and a clear regulatory framework at a pan-European level. Indicatively, it is stated that Article 13 of the Security Council applies to the exchange and promotion of personal data.

However, Authentication Platforms (e-AU, e-ID, e-SIGN), in conjunction with the emerging technologies that have emerged below, have set up a strong security framework, which of course needs to be constantly revised as network security threats (cyber terrorism, cyber espionage), advanced permanent threats, mixed threats, etc.) are constantly changing as vulnerabilities are discovered in both established and newly established systems and solutions are needed to address these threats.

It is obvious that the existing technological achievements could ideally be applied in the field of e-agriculture, especially in precision agriculture. The US Federal Bureau of Investigation (FBI) has released a guide that draws attention to the dangers posed by the increasing use of technology in Smart Georgia. Precision Agriculture generates huge amounts of data and related security crises. There are challenges regarding the use of data, storage method and ownership. Even since the early introduction of data generating precision agricultural data, there have been concerns from farmers themselves about how and where the data is stored and used. The data extracted by farmers are just as sensitive as other sectors and contain personal data of producers and their staff. Some of these may be the financial status of the farms concerned, crop yield data, property sites, and more. One proposed solution is the use

of Ciphertext (CP-ABE) policy-based encryption, which could be applied not only to e-farming systems but to all cross-border government systems [27] [29].

3.4 Privacy

Cross-border electronic services should ensure a uniform level of protection of personal data, including measures, in which individuals have the right to choose whether their data can be used for purposes other than their original use. Data processing information should also be provided to anyone interested. However, all the above and the work on interoperability should be in line with the latest General Data Protection Regulation (GDPR), which was issued on 25 May 2018.

3.5 Subsidiarity

The guidance provided by the European Interoperability Framework concerns only the cross-border level of services. In accordance with this principle of subsidiarity, this guidance does not affect the internal functioning of administrations and national agencies, and each EU Member State should accommodate the necessary measures to ensure the subsidiarity of its systems across borders [25].

3.6 Policy and Regulation

A spectrum of new guidelines, policies, laws and governmental changes is needed for the pursuit of cross border e-government systems principles in order to address electronic activities including archiving, signatures, identification, data protection, intellectual property rights and copyright matters.

The forming of protections and legal amendments will be required in order to ensure in addition to further elements, privacy, security and legal acknowledgement of electronic signatures and interactions. A holistic approach which is not focused solely on technology must be incorporated for this effort to be successful. Similarly, new policy conditions and legal reforms may have to be embraced before the smooth functionality of the online world. Significant project complication or stopper can be caused by archaic laws, old regimes of regulation and contradictory authorities.

4 Discussion

Cross-border government services have been at the forefront for a number of years now and all indicate that they will be at the spearhead in the future as they offer significant advances in further development of applications in almost all areas and Life Sciences applications such as health, agriculture, justice, commerce and etc. However, key enablers for further penetration of cross-border e-services are security, personal data protection and interoperability. Meanwhile, ready-made authentication

platforms (e-AU, e-ID, e-SIGN), in combination with emerging technologies (CC, IoT, BD and AI) offer basic conditions for additional development in specific data-specific application areas, such as e-agriculture, namely precision agriculture.

Interoperability between Member States' public administrations is a prerequisite for the provision of cross-border services. Accessibility, multilingualism, security, subsidiarity, the use of open standards and the protection of personal data are the principles of well-functioning systems and at the same time, the reason for upgrading existing systems to smart ones.

Although in recent years a multitude of European programs and initiatives have been implemented to mature the existing cross-border systems technologically and institutionally, a lot remains to be done in order to remove obstacles and address the issues of cross-border systems and e-government services.

References

1. Sideridis, A. B., Protopappas, L.: 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 (2015).
2. European Commission, 2010, The European eGovernment Action Plan 2011-2015-Harnessing ICT to promote smart, sustainable & innovative Government in ICT for Government and Public Services 2010. Brussels: EC publications. <http://eur-lex.europa.eu/legal-content/EN/TXT>
3. Gouscos D., Mentzas G.: PASSPORT - A Novel Architectural Model for the Provision of Seamless Cross-Border e-Government Services. DEXA conference, Workshop on Electronic Government, Munich (2001).
4. Commission of the European Communities, eEurope: An Information Society For All, Communication on a Commission Initiative for the Special European Council of Lisbon, March 23-24, (Accessed 22/07/2020).
5. European Commission: [online] <https://ec.europa.eu/cefdigital/wiki/display/CEF+DIGITAL/2018/10/25/TOOP%3A+The+Once-Only+Principle> (Accessed 6/07/2020).
6. European Interoperability Framework For Pan-European eGovernment Services.: [online] Brussels, (2004), <http://ec.europa.eu/idabc/servlets/Docd552.pdf?id=19529/> (Accessed 03/07/2020).
7. European Patients - Smart open Services, epSOS.: [online] <http://www.epsos.eu/> (Accessed 12/07/2020).
8. Sideridis, A. B.: A Smart Cross Border e-Gov Primary Health Care Medical Service. International Conference on e-Democracy 2019, Athens (2019).
9. Sideridis, A. B., Protopappas, L., Tsiafoulis, S., Pimenidis, E.: Smart Cross - Border e-Gov Systems and Applications. In: Proceedings of the 6th E-Democracy Conference. 151-168, Athens, Greece (2015).

10. Interreg Europe: [online] <https://interreg.eu/programme/interreg-europe/> (Accessed 03/07/2020).
11. European Commission: [online] https://ec.europa.eu/regional_policy/en/policy/cooperation/european-territorial/egtc/ (Accessed 19/06/2020).
12. Pimenidis, E. and Georgiadis, C.K.: Can e-Government Applications Contribute to Performance Improvement in Public Administration?, *International Journal of Operations Research and Information Systems*, 5(1), p. 48-57 (2014).
13. Lenz, T., & Zwattendorfer, B.: Towards Cross-Border Authorization in European eID Federations. In *Trustcom / BigDataSE/I SPA, 2016 IEEE* (pp. 426-434). IEEE (2016).
14. STORK 2.0., [online] http://www.ehgi.eu/Lists/Posts/Attachments/12/Day1_3_STORK%20on%20eID_Robert%20Scharinger.pdf (Accessed 22/06/2020).
15. STORK 1.0 (b) [online] eID Consortium, D2.3 Quality authenticator schem. <http://www.eid-stork.eu/> (Accessed 11/06/2020).
16. STORK 2.0 eID Consortium, D5.1.1 eLearning Pilot Technical Business Objectives and Specifications, www.eid-stork2.eu, 2013.
17. Leitold, Herbert, Bernd Zwattendorfer, "STORK: Architecture, Implementation and Pilots", *ISSE 2010 Securing Electronic Business Processes*, pp 131-142 (2010).
18. Sideridis A. B., Protopappas L., Tsiafoulis S. and Pimenidis E. : Smart Cross-Border e-Gov Systems and Applications, *Proceedings of the 6th EDemocracy Conference (e-Democracy 2015)*, Athens, Greece, 10-11 December 2015, pp. 151-168 (2015).
19. IDABC and EIF, *European Interoperability Framework for Pan – European E-Government Services*, Belgium (2004)
20. Sideridis, A. B., Protopappas, L., Tsiafoulis, S., Pimenidis, E.: Smart Cross - Border e-Gov Systems: an application to refugee mobility. To appear in the *International Journal of Electronic Governance* (2017)
21. European Parliament and the Council of the European Union.: Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC 27. In: *Official Journal of the European Union*, L 257/73, Brussels (2014)
22. European Commission: [online] <https://ec.europa.eu/digital-single-market/en/trust-services-and-eid> (Accessed 15/06/2020).
23. Sideridis, A. B.: Smart Cross Border e-Government Systems and their application to e-Agriculture. To appear in special volume in honor of Prof. A. Karamanos, editor: *Agriculture University of Athens*, Athens, Greece (in Greek) (2017).
24. Sideridis, A. B., Pimenidis, E., Costopoulou, K., Yialouris, C. P., Savvas, I., Maliappis, M., Ntaliani, M., Karetzos, S., Tsiafoulis, S., Protopappas, L., Chatziandreou, A.: e-Gov: In: *Proceedings of Recent Advances in Life Sciences & EE's Project Proposals (Medical, Animal, Plant, Food Sciences and Environmental Protection)*, Doctoral Concorcium, HAICTA 2017. Chania, Crete (2017).

25. Tauber A., Zefferer T., Zwattendorfer B.: Approaching the Challenge of eID Interoperability: An Austrian Perspective, *European Journal of ePractice*, No 14, pp. 22-39 (2012).
26. European Interoperability Framework For Pan-European eGovernment Services, 2004: Belgium. [online] <http://ec.europa.eu/idabc/servlets/Docd552.pdf?id=19529/> (Accessed 03/06/2020).
27. Xu, F. J., Zhao, V. P., Shan, L., & Huang, C.: 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 (2014).
28. European Commission: [online] https://ec.europa.eu/info/law/law-topic/data-protection_en (Accessed 30/06/2020).
29. Tomaszycski K.: The interoperability of European information systems for border and migration management and for ensuring security. Faculty of Law, University of Bialystok (2019).
30. European Commission [online] https://ec.europa.eu/isa2/sites/isa/files/public_multilingual_knowledge_management.pdf (Accessed 23/07/2020).
31. AthexGROUP: [online] <https://www.athexgroup.gr/el/web/guest/digital-certificates> (Accessed 25/07/2020).
32. Gerakos K., Malippis M., Costopoulou C., Ntaliani M.: Electronic Authentication for University Transactions using eIDAS. 7th International Conference, E-Democracy 2017, Athens, Greece, December 14-15 (2019).
33. Publication Office of European Union : [online] <https://op.europa.eu/en/publication-detail/-/publication/1f1b9793-81bb-11e9-9f05-01aa75ed71a1> (Accessed 25/07/2020).
34. European Commission: [online] <https://ec.europa.eu/futurium/en/egovernment/agriculture-and-egovernment-project-eidas> (Accessed 24/07/2020).
35. Behl, A., Behl, K.: Security paradigms for cloud computing. In: 4th International Conference on Computational Intelligence, Communication Systems and Networks, pp. 200–205. IEEE (2012)