Feasibility and implementation study on the incorporation of the provisions related to trust services of the eIDAS Regulation to Hellenic e-Government environment

Leon Evangeliou MTE14008

SUPERVISED BY PROF. S. KATSIKAS

M.Sc. Techno-economic Analysis and Security of Digital Systems

University of Piraeus

30/6/17

Abstract

This dissertation investigates the exploitation prospects of the eIDAS Regulation's eID, electronic documents, and electronic trust services by the Hellenic e-Government environment. eIDAS facilitates the creation of a single digital market for the EU by promoting technical interoperability and security levels in relation to eID means and trust services applicable to electronic transactions. When implemented in the Hellenic e-Government environment, it would be possible to assure secure, trustworthy, and convenient access to online resources from any location in the EU. Consequently, the Greek Government will be able to offer superior and innovative online services to its citizens. Based on the findings, the www.ermis.gov.gr and www.gsis.gr portals appear to fit, as they are, into the eIDAS regulatory framework. An outcome-based approach is proposed to facilitate secure and reliable online services. Here, the security goals of the eIDAS interoperability framework that is based on mutual recognition and notification among other principles are prioritised at the expense of relying too much on technology. From management and policy perspectives, policymakers in Greece should ensure they comply with all the requirements of eIDAS for successful implementation of the regulation in the e-Government portals.

Contents

To the memory of my grandfather Wally who made studying this degree possible,

to my supervisor Dr. Katsikas and my parents.

1.0 Introduction

Over the years, the EU market has been facing security and privacy challenges in relation to electronic transactions and electronic signatures as users conduct their business processes online. In fact, data/information security breaches remain a major threat to successful electronic funds transfer (EFT) transactions among mobile and Web-based processes to-date[1]. In addition, inadequate compatibility, accessibility, and transparency of standards for electronic identification, authentication and trusted services have been identified as factors inhibiting digital growth and innovation in the EU. For example, it is difficult for a member state to recognise an electronic identification system based on a framework different from what it uses[2]. Therefore, security and privacy, compatibility, accessibility, and transparency issues are key inhibitor to sustained digital development and innovation in the EU.

With growing concerns of digital growth, innovation, and information security, electronic IDentification, Authentication and trust Services (eIDAS) was established by the European Commission as a regulation to promote the European digital agenda. This regulation covers aspects of electronic identification, trust services, and electronic documents used by EU member states to ensure secure cross-border business. It provides member states with trusted services (especially electronic signatures, time stamps, and seals, electronic registered delivery

---

[1] eur-lex.europa.eu, *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*, [website], 2014, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG, (accessed 11 October 2017).

[2] eid.as, *eIDAS – The Ecosystem*, [website], 2017, https://www.eid.as/home, (accessed 9 October 2017).

services, and certificates for website authentication), which may be readily assessed within the integrated EU signing framework. Consequently, security stakeholders are better placed to make more informed decisions when securing electronic signatures[3]. Therefore, all member states must recognise and use electronic identification and authentication mechanisms as well as trust services that comply with eIDAS standards as required by EU regulations for digital growth and prosperous Europe.

This is a feasibility and implementation study on the incorporation of the provisions related to trust services of the eIDAS Regulation to Hellenic e-Government environment.

[3] Ibid., 1.

1.1 Research background

In the European Union (EU), regulations constitute legal acts that are binding or enforceable immediately and in their entirety across every member state. Other than regulations, the EU makes directives and decisions as legally binding requirements in addition to opinions and recommendations that are not enforceable. Regulations mainly differ from directives, decisions, opinions, and recommendations in that the later requirements are only applicable to member states to which they are addressed[4][5]. Fundamentally, the five broad categories of EU requirements are aimed at exercising and strengthening the competences of the Union[6].

The following are the subclasses of EU regulations: Commission Implementing Regulation, Regulation of the European Parliament and of the Council, Council Regulation, and Commission Regulation. It should be noted that EU regulations may be implemented into national laws through different legislative measures and procedures based on their specific subject matter[7]. Therefore, member states are required to mediate the Union's regulations into their existing laws that deal with the related subject matter. This makes regulations one of the fundamental forces of the EU law. eIDAS was established in the EU Regulation No. 910/2014 on electronic identification standards in September 2014 to deal with the 'electronic identification and trust services' for European market's electronic transactions. Most articles in the eIDAS came into

---

4 M. Horspool, Matthew Humphreys and Michael Wells-Greco, *European Union Law* (Oxford University Press, 2016).

5 C. F. Bergström and Dominique Ritleng, *Rulemaking by the European Commission: The New System for Delegation of Powers* (Oxford University Press, 2016).

6 Ibid. 45.

7 Horspool, Matthew Humphreys and Michael Wells-Greco, op. cit. 16.

effect on 1st July 2016 to repeal the 1999/93/EC Directive that aimed at creating a centralised electronic signing platform for EU member states[8].

eIDAS provides a collection of identification and authentication standards that make cross-border electronic transactions to have the legal standing similar to that of paper-based transactions such as conventional facsimile and mail services. Common mechanisms pushed by this regulation include advanced electronic signatures, qualified electronic signatures, trust services, and qualified digital certificates[9][10]. An advanced electronic signature must meet the following requirements: be solely created and controlled by its signatory, capably provide unique information that identifies its signatory, identify any change to data sent with the message after being digitally signed, and invalidate any signature in case of a change to data[11]. eIDAS requires electronic signatures that are based on qualified digital certificates to authenticate that a qualified trust service provider issued the certificate in question. The provider handles trust services – digital services that create, validate, and verify authentication mechanisms like electronic signatures, seals, timestamps, and certificates[12]. Qualified electronic signatures are basically advanced electronic signatures technically created by 'qualified electronic signature creation devices'[13].

---

8 eur-lex.europa.eu, op. cit. 1.

9 docusign.com, What is the eIDAS Regulation?, [website], 2017, https://www.docusign.com/learn/eidas, (accessed 11 October 2017).

10 eur-lex.europa.eu, op. cit. 1.

11 eid.as, op. cit. 1.

12 eur-lex.europa.eu, op. cit. 1.

13 eid.as, op. cit. 1.

Starting 1st July 2016, eIDAS requires qualified electronic signatures to be accorded the legal effect equivalent to handwritten signatures. In addition, it covers electronic seals that are applied to digital documents to assure their authenticity and integrity. Time stamping incorporates the date and time elements on digital documents to indicate existence at a specific point in time. Some trust services authenticate websites by providing trusted information like certificates on a site to allow visitors to identify the owner[14]. Therefore, eIDAS was effected to enhance the seamlessness, security, and confidentiality of electronic transactions in the EU market.

[14] J. Bender, *eIDAS Regulation: eID – Opportunities and Risks*, 2015, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/SmartCard_Workshop/Workshop_2015_Bender.pdf?__blob=publicationFile, (accessed 10 October 2017).

1.2 Research problem

While the EU formally adopted eIDAS in July 2014, implementing legally-compliant technologies and procedures has seen a lot of debate and innovation related to best practises[15]. In the context of the Hellenic e-Government environment and associated electronic transactions, eIDAS stands to drive the highly sought after digital growth as well as innovation. Legacy, less secure digital solutions and emerging ones that have not been adequately tested may not suffice in matters of improved innovation and information security. eIDAS Regulation in general can possibly suffice as it pushes organisations to pursue the highest possible innovation and security levels. However, the revocation of the 1999/93/EC Directive for authentication in favour of eIDAS has not been accompanied by widespread implementation of trust services required by the new regulation. Even though the Hellenic e-Government portals - www.ermis.gov.gr and www.gsis.gr comply with the 1999/93/EC Directive for authentication, they do not completely support the trust services introduced by the eIDAS Regulation. This incurs a number of unanswered questions. To start off, how feasible and effective would eIDAS be with respect to supporting realisation of a highly innovative and secure Hellenic e-Government environment for public administration? What are eIDAS limitations? And, which roadmap should the Hellenic e-Government stakeholders adopt at management, policy, and technical levels for successful implementation of appropriate eIDAS trust services?

[15] eid.as, op. cit. 1.

1.3 Research aim and objectives

Currently, the Hellenic e-Government portals, www.ermis.gov.gr for public administration and www.gsis.gr for registration procedures of the General Secretary of Information Systems use the already repealed 1999/93/EC Authentication Directive. However, the entire e-Government platform does not fully support the entire eIDAS's trust services. The aim of this research is to investigate the feasibility and process of implementing the provisions related to trust services of the eIDAS Regulation to Hellenic e-Government environment.

The following are the objectives of this study:

1. To critically evaluate potential eIDAS opportunities and limitations.
2. To critically evaluate the exploitation prospects of the eIDAS Regulation’s trust services with respect to the Hellenic e-Government environment.
3. To propose a roadmap at management, policy and technological levels for implementation of the eIDAS Regulation’s trust services at the Hellenic e-Government environment.

1.4 Significance of this research

Electronic trust services (e.g. electronic signatures and electronic seals) have emerged as suitable solutions to help carry out secure cross-border electronic transactions, while assuring greater efficiencies in terms of costs and time. They assure individuals and organisations executing huge amounts of electronic transactions higher accuracies of content and date/time as well as legal certainty. However, a lack of a universal set of legally valid trust services for the EU digital market opens a door for electronic transactions and processes to be challenged in courts. Moreover, they increase the likelihood of exposure to cybersecurity threats, especially data breaches and fraudulent activities while processing, storing and distributing huge amounts of data. For example, a mere electronic seal does not prevent unauthorised data access. Instead, qualified electronic seals may be used to improve the security of electronic transactions as well as data confidentiality and integrity[16]. Therefore, there is need for more secure, reliable and trustworthy electronic trust services as mandated by the eIDAS Regulation to spur sustained growth of the EU digital economy.

Electronic signatures have been critical to national, regional and global electronic transactions for many years, and regulatory agencies and businesses are continuously demonstrating notable interest in sustained advancements in the field[17]. eIDAS has become a popularly

---

[16] Katehakis, Dimitrios G., George Pangalos, and Andriana Prentza, 'Security Improvements for Better and Safer Cross-Border ePrescription and Patient Summary Services', *International Journal of Reliable and Quality E-Healthcare (IJRQEH)*, 6/1 (2017), 18-28.

[17] M. Alexander, Thomas Zefferer, Florian Reimair, Çağatay Karabat, and Elif Ustundag Soykan, Leveraging the adoption of electronic identities and electronic-signature solutions in Europe, In *Proceedings of the Symposium on Applied Computing*, pp. 69-71 (ACM, 2017).

debated and researched issue among commercial and non-profit organisations in the EU. It mainly covers identification and trust services for secure, reliable and seamless cross-border electronic transactions. eIDAS is crucial to the creation of legally-compliant electronic signatures. In addition, it forms an integral part of the greater technological innovation as well as economic and social growth in the EU[18]. However, best practises regarding implementation of eIDAS-compliant technologies and processes are still being largely developed and debated[19]. Therefore, senior organisational leadership and information security personnel should understand the regulation and its implications for their businesses, especially in terms of economic growth and technological investments.

The study of the feasibility and potential implementation of the provisions related to trust services of the eIDAS Regulation to Hellenic e-Government environment contributes to the general field of electronic transactions and electronic identification, authentication, and trust services. Moreover, it provides practical recommendations to the Hellenic e-Government stakeholders in relation to best practises and policies for successful implementation of eIDAS-compliant trust services and associated technologies and processes. Consequently, the findings of this study contribute to the implementation of the eIDAS Regulation into Hellenic national laws as a mandatory legal requirement of the European Commission.

---

[18] B. Jérôme, Marianne Fraefel, and Reinhard Riedl, Raising Acceptance of Cross-Border eID Federation in e-Government and e-Business, In *European Conference on e-Government* (Academic Conferences International Limited, 2014).

[19] Průša, Jiří, 'E-identity: Basic building block of e-Government', In *IST-Africa Conference*, *2015*, pp. 1-10 (IEEE, 2015).

1.5 Organisation of this thesis

In Chapter 1.0: Introduction, the research topic was introduced and the research background, problem, and aim and objectives presented. In addition, the Chapter demonstrates the significance of this research, including theoretical and practical contributions.

The rest of this thesis report is organised into the following major Chapters:

- Chapter 2.0: Literature Review: A comprehensive review of past literature related to the eIDAS Regulation and its feasibility and implementation issues.
- Chapter 3.0: Research Methodology: A description of the adopted research methods.
- Chapter 4.0: Results and Discussion: A summary of the study findings and a discussion of the findings obtained from the study as indicated by reviewed literature, while paying close attention to the research aim and objectives, context of current literature, and theoretical and practical implications with respect to the eIDAS Regulation and its implementation at the Hellenic e-Government environment.
- Chapter 5.0: Conclusion and Recommendations: A synthesis and integration of broader issues raised in the report. It also recommends an appropriate course of action and further study considerations.

2.0 Literature Review

2.1 Introduction

The eIDAS Regulation offers predictability in EU regulations to facilitate seamless, secure, and reliable electronic transactions between citizens, public agencies and businesses. The regulation in this regard ensures that individuals and organisations can access a collection of public services provided by other EU member states. Every EU nation need to avail its electronic identification system (eIDs) to others for greater accessibility to the services[20]. Fundamentally, eIDAS has established an EU market for a number of electronic trust services, particularly electronic signatures, time stamps, electronic delivery services, website authentication, and electronic seals. It enables these services by ensuring that they are functional across EU member states and are legally admissible just like conventional paper-based processes[21]. This chapter entails an in-depth literature review to unearth what past studies say regarding the research topic. In addition, it has defined a number of fundamental terms and explored prevalent theories related to the research topic.

---

[20] eur-lex.europa.eu, op. cit. 1.

[21] eid.as, op. cit. 1.

2.2 Online platforms and their role in social and economic development

Online platforms attract increasingly growing attention, especially from regulatory agencies for their role in promoting the digital economy[22]. However, it is worth defining what an online platform means. Research indicates that these platforms differ strikingly in terms of the business model, sector, size, activity, and security and privacy requirements associated with each platform. As such, the current regulatory framework treats them with indeterminate plurality and generality[23]. Adoption and usage trends of online platforms remain consistent in Germany, UK, Spain, France, Poland and other European countries, with information platforms (for searching for opportunities and looking up information) and communication tools (for purposes like interacting with family and friends) being the most prevalent types[24].

The online environment presents lucrative opportunities for a sustainable digital economy in Europe and beyond, driving benefits for both businesses and consumers. For example, research has shown that online platforms promote communication, entertainment, product and service comparison, online marketplaces, and information access[25]. For example, with advancements in Web and mobile technologies, communicating and engaging with contacts such as family members and friends has become easier. Moreover, accessing and sharing videos, music, games, photos, and other types of content has been made easier by online entertainment

---

[22] World Bank, *Doing Business 2015: Going Beyond Efficiency* (World Bank Publications, 2014).

[23] C. Rule, *Online Dispute Resolution For Business: B2B, ECommerce, Consumer, Employment, Insurance, and other Commercial Conflicts* (John Wiley & Sons, 2003).

[24] Ibid. 50.

[25] World Bank op. cit. 16.

platforms. Businesses have also launched online marketplaces for selling and buying products and services[26].

Internet users believe that online platforms lead to improved transparency and cost- and time-efficiencies, greater transparency, and increased options[27]. Case studies of businesses have shown that the digital environment drive value in the following key areas: e-commerce (e.g. online shopping and payment, after-sales follow-ups, and shipping), marketing (e.g. marketing campaigns and product development), resourcing (e.g. solicitation for project funding), and professional networking (e.g. job vacancy advertisements and career advice)[28]. In addition, online platforms have considerably reduced geographic barriers as well as cost structures to the benefit of businesses and customers[29].

---

[26] L. In, *Electronic Commerce Management for Business Activities and Global Enterprises: Competitive Advantages: Competitive Advantages* (IGI Global, 2012).

[27] M. Andreas and Henrik Stormer. *eBusiness & eCommerce: managing the digital value chain* (Springer Science & Business Media, 2009).

[28] World Bank op. cit. 32.

[29] Xiaoming Zhu, Bingying Song, Yingzi Ni, Yifan Ren, Rui Li, *Business Trends in the Digital Era: Evolution of Theories and Applications* (Springer, 2016).

2.3 Managing identity across online platforms

The ever-growing emergence of online platforms has changed the way the identity of entities such as citizens, customers or organisations transacting over the Internet is established, verified and validated prior to allowing access to services provided by public authorities and businesses for security, reliability, and trust purposes[30]. Improvements in electronic identification systems and processes have emerged as a fundamental concern for European states in their pursuit of better relationships and interactions between governments and citizens (G2C), businesses and consumers (B2C), and businesses and employees (B2E)[31]. Specific regulations are being established to ensure that electronic signatures provide a legal standing equivalent to that of handwritten signatures. eIDAS and NIST-DSS for the EU and USA respectively are examples of such regulations. Contrary to digital signatures that are based on cryptographic algorithms, electronic signatures may be simply a name typed into an electronic document as a means of identification[32]. This way, it is possible to authenticate for electronic services as well as benefits.

---

[30] Průša, Jiří, 'E-identity: Basic building block of e-Government', In *IST-Africa Conference*, *2015*, pp. 1-10 (IEEE, 2015).

[31] R. Kai, Denis Royer and André Deuker, *The future of identity in the information society: Challenges and opportunities* (Springer Science & Business Media, 2009).

[32] Tsatsou Panayiota, Silvia Elaluf-Calderwood, and Jonathan Liebenau, 'Towards a taxonomy for regulatory issues in a digital business ecosystem in the EU,' *Journal of Information Technology*, 25/3 (2010), 288-307.

2.4 The eIDAS Regulation and electronic trust services

The eIDAS Regulation basically establishes a cross-border and cross-sector legal framework that covers electronic signatures, electronic documents, electronic time stamps, electronic seals, certificate services (for authentication of websites), and electronic registered delivery services in relation to eIDs and EU-based trust service providers. Before reviewing what the regulation requires, it is important to define a number of terminologies. To start with, eIDAS is a system designed to facilitate electronic identification and it forms the basis for issuing electronic identification means to persons. Trust services are electronic services that are normally offered for payment, and comprise of the creation, verification, validation, and preservation of electronic forms of signatures, time stamps, registered delivery services, and associated certificates. Electronic identification entails use of electronic person identification data to uniquely represent a person – either a human being or an organisation. Person identification data is a collection of data that enable the identity of a person to be confirmed or ascertained. Electronic identification means imply a unit (either material or immaterial) holding person identification data to facilitate authentication for online services[33]. Here, authentication means enabling electronic identification of a person or establishing the source and integrity of electronic data.

. A signatory uses this data to sign and ensure the source and integrity of the latter form of data. An electronic registered delivery service is a service enabling electronic transmission of data between third parties, while providing evidence such as proof of data sending and receipt. In addition, it prevents common risks, including loss, leakage, theft, destruction, or

[33] eur-lex.europa.eu, op. cit. 1.

unauthorised modification. A certificate for website authentication is a confirmation enabling authentication for a website by linking it to the entity that is issued with the certificate. eIDAS also introduces additional constraints like advanced electronic signature, qualified electronic signature, certificate for electronic signature, qualified certificate for electronic signature, and qualified trust service which are defined in its different articles. Trust services and products (hardware and software systems used to deliver the services) that comply with eIDAS are allowed to freely circulate in the Union[34].

EU member states are allowed to establish eIDs of their choice for granting access to online services, including the possibility of involving private organisations in the delivery of the means. Existing national provisions may be maintained, or new ones introduced to assure conformity with the EU law. The eIDAS Regulation establishes the principle of mutually recognised electronic identification and authentication for online services. It concerns eIDs communicated by member states as well as trust service providers established within EU. Here, authentication to be granted service access concerns processing of identification details that are relevant and sufficient as opposed to excessive information. Moreover, regulatory authorities and trust service providers are required to uphold the security and privacy of processing[35]. The regulation eliminates existing barriers to use of eID means across European countries to authenticate for public services at minimum[36]. Therefore, it assures cross-border access to online services

---

[34] eur-lex.europa.eu, op. cit. 1.

[35] Sid, Alexander B., Loucas Protopappas, Stergios Tsiafoulis, and Elias Pimenidis, Smart cross-border e-gov systems and applications, In *International Conference on e-Democracy*, pp. 151-165 (Springer, Cham, 2015).

[36] Tsatsou Panayiota, Silvia Elaluf-Calderwood, and Jonathan Liebenau, op. cit. 301.

provided by EU members within the constraints of secure, safe, and trustworthy electronic identification and authentication. More precisely, mutual recognition as required by the regulation only covers authentication for online services. National legislation sets out the conditions under which the services may be accessed and eventually delivered to applicants based on applicable rights[37].

Other than the conventional trust services, the eIDAS regulation introduces 'advanced' and 'qualified' forms of trust services that come with additional requirements. For example, an electronic signature basically means electronic data a signatory uses to sign digital data as evidence of approval or acceptance. However, can the signatory be identified? Can another person other than the legitimate signatory use the signature creation data to sign? Can changes to signed data be detected? An advanced electronic signature seeks to address these issues by ensuring that an electronic signature is uniquely associated with signatory; sufficient to identify the signatory; created using data under sole control of the signer; and tied to what has been signed so as to detect illegal or unauthorised changes. eIDAS further requires a qualified electronic signature – an advanced signature with a legal status equivalent to that of a handwritten signature. To achieve this status, the signature must be accompanied with a qualified certificate that is issued by certified trust service providers after verifying and validating the signatory's identity and the signature's authenticity. This also applies to electronic seals, registered delivery services, time stamps, and website authentication certificates whereas the identity of the signatory, sender, addressee and site owner are highly

---

[37] eur-lex.europa.eu, op. cit. 1.

prioritised[38]. In the case of a qualified electronic registered service, a qualified electronic signature, seal and time stamp are required to bolster security and integrity[39]. This way, eIDAS plays a critical role in determining the admissibility of trust services as evidence across the EU regardless of their electronic forms. For example, a qualified electronic signature compliant with several EU standards like being regulated by a member state and accompanied by an appropriate qualified certificate attached to an email is highly likely to pass the legal test than a merely typed name.

eIDAS strives to promote technology neutrality. Nevertheless, it requires qualified trust service providers (TSPs) to meet a set of technical standards so that they can be included on the 'EU Trusted List'. These standards include specifications for various eIDAS-defined forms of electronic signatures, certification and control of TSPs, and eID and their associated assurance levels[40]. Online services require different identity assurance levels for access to be granted. Members are obliged to recognise eIDs whose electronic identification means characterise substantial assurance or confidence that the individual claiming a certain identity is indeed the one with the assigned identity[41]. This way, it is possible to electronically control access to online services without geographical barriers.

Electronic identification and identity assurance levels put into consideration processes (such as identity verification and authentication), monitoring and control entities (such as the providers of electronic identification services), and deployed technical measures. Under eIDAS, the basic

---

38 Tsatsou Panayiota, Silvia Elaluf-Calderwood, and Jonathan Liebenau, op. cit. 303.
39 eur-lex.europa.eu, op. cit. 1.
40 docusign.com, op. cit. 1.
41 Tsatsou Panayiota, Silvia Elaluf-Calderwood, and Jonathan Liebenau op. cit. 307.

assurance levels are 2 (low), 3 (substantial) and 4 (high) as outlined by EU-sponsored Large-Scale Pilots (like STORK) and standardisation initiatives (like ISO 29115). The levels specify the minimum technical standards and requirements that should be considered to comply with the regulation and ensure it is applied consistently. Moreover, implemented eIDs and related identification means should not be tied to a specific technology to ensure interoperability[42]. Private organisations, regardless of where their nation where they are based, are encouraged to rely on electronic identification means that fall under notified schemes for electronic transactions[43]. When this is practised by all EU member states, especially for online public services, it may help citizens and businesses access the services without overly restrictive geographical barriers.

---

42 eur-lex.europa.eu, op. cit. 1.

43 R. Kai, Denis Royer and André Deuker, op. cit. 59.

2.5 The eID ecosystem

A typical eID ecosystem comprises of five key components, namely the member states, node operators or connection points (member states), attribute and identity providers that provide information related to electronic identities and that verify user identities, service providers that offer online services whose access is authenticated through eID, and citizens. eIDAS defines citizens as persons and organisations that seek online services from any EU member state using their domestic eID with assured security, cost- and time-efficiencies, and usability[44].

[44] Elizabeth, Kennedy, and Christopher Millard, 'Data security and multi-factor authentication: Analysis of requirements under EU law and in selected EU Member States', *Computer Law & Security Review*, 32/1 (2016), 91-110.

2.6 Interoperability

Notifying and receiving member states have different integration models to choose from when it comes to eIDs. Notifying states may use the proxy-based model to relay authentication data between receiving states and their eIDs. Alternatively, they may use the middleware-based model by providing a middleware to other EU nations. The receiving member states operate the middleware. Similarly, the receiving member states may adopt a centralised or decentralised model. In the former, the receiving state has a single centralised instance of the software that supports interoperability. The software receives identity data from other eIDs and forwards it to trust service providers operating in that state. On the other hand, receiving states may adopt the decentralised model whereas service providers directly instantiate the interoperability software. Each of these variants of interoperability models for notifying and receiving sides has several risks. From the notifying side, the proxy-based implementation must establish a single centralised instance of interoperability to enable the monitoring of outbound authentications of citizens from a shared identity provider. This implies a potential single point-of-failure, which is not the case with the middleware architecture that comes with the need for different middleware implementations for every eIDs as the only major disadvantage. However, it is possible to mitigate this problem by ensuring that different eIDs are based on the same interoperability technology. On the other hand, the receiving side, the centralised deployment comes with higher IT security and privacy risks because a central interoperability instance forms a highly valuable target for attackers. The completely decentralised architecture for receiving

states distributes personal identification data across several service providers, thus there is reduced likelihood of cybersecurity attacks[45].

[45] Bender, op. cit. 159.

2.7 The role of eIDAS in electronic transactions

Online platforms and processes must have adequate trust for them to drive the much anticipated sustainable social and economic development in EU. Lack of sufficient trust, to a larger extent due to challenged legal and regulatory certainty, continue to inhibit adoption of electronic transactions and new services by public authorities, businesses, and consumers[46]. In 2010, the Europe's 'Digital Agenda' identified several factors that inhibited the internal digital economy and markets. These included the surging cybersecurity incidents, poor interoperability, and intensive fragmentation[47].

The already repealed 1999/93/EC Directive covered electronic signatures, but it did not deliver an in-depth 'cross-border and cross-sector' regulatory framework for supporting trustworthy, secure, easy-to-use, and reliable electronic transactions conducted in the EU. Moreover, electronic identification, authentication, and signatures are required for most online services accessed through 'points of single contact' established by different EU members[48]. Mostly, the national eIDs of various EU member states are different, thus citizens face difficulties authenticating themselves across borders since their eID may be unrecognised in foreign countries. Lack of mutually recognised eID also makes it difficult for public authorities to provide their online services, especially in the cross-border context. The barrier to electronic

---

[46] M. Alexander, Thomas Zefferer, Florian Reimair, Çağatay Karabat, and Elif Ustundag Soykan, Leveraging the adoption of electronic identities and electronic-signature solutions in Europe, In *Proceedings of the Symposium on Applied Computing*, pp. 69-71 (ACM, 2017).

[47] B. Jérôme, Marianne Fraefel, and Reinhard Riedl, Raising Acceptance of Cross-Border eID Federation in e-Government and e-Business, In *European Conference on e-Government* (Academic Conferences International Limited, 2014).

[48] Průša, Jiří, op. cit. 6.

identification implies that service providers and consumers do not optimise the offerings of the EU digital market[49]. For example, lack of a common eID and authentication framework limits the transferability of electronic documents across borders mainly because of security and trustworthiness issues. As a result, the EU citizens are deprived of their rights to enjoy the benefits related to cross-border digital market and services. So, there was need to come up with an EU regulation that would improve and expand the legislation and legal acts that constitute the Union's body of law[50].

The European Commission created the eIDAS Regulation to facilitate the creation of a single digital market for the EU while ensuring adequate security levels in relation to eID means and trust services applicable to electronic transactions. In fact, rolling out the regulation implies greater levels of security and convenience for online activities like submitting tax returns, college enrolment, authenticating for online payment, establishing business across borders, remotely running a bank account and others[51]. Basically, the regulation implies improved trust levels in electronic transactions by offering a shared environment for conducting secure and reliable electronic interactions between public authorities, businesses, and citizens. With enhanced trust, it is expected that the overall effectiveness and efficiency of 'cross-border and

---

[49] Sid, Alexander B., Loucas Protopappas, Stergios Tsiafoulis, and Elias Pimenidis, op. cit. 155.

[50] Průša, Jiří, op. cit. 8.

[51] ec.europa.eu, *Trust Services and eID*, [website], 2017, https://ec.europa.eu/digital-single-market/en/trust-services-and-eid, (accessed 18 October 2017).

cross-sector' online services and electronic business and/or commerce in EU will be greatly improved[52].

Notably, stakeholders highlighted the need to have an appropriate environment for mutual recognition or acknowledgement of main enablers across the EU member states. Interoperable, trustworthy, and secure electronic identification, electronic signatures, electronic delivery services, electronic documents and records, electronic seals, and time stamps and e-government services are some of the key enablers identified by the Commission[53]. Electronic signatures and a public key system that serve the entire EU are critical to running secure electronic services. A common validation authority gateway for EU members would assure cross-border compatibility of diverse electronic signatures. In addition, it would enhance the security and trustworthiness of Internet-based transactions whereas trust services may be used as legal evidence is the Union[54].

Electronic trust services drive considerable cost and time savings in relation to high-volume and cross-border electronic transactions. Consequently, it is possible to concurrently work on an electronic document regardless of the geographical place where signatories are located. Civic organisations in the EU would automatically process several electronic documents and use services like qualified electronic seals for secure sealing purposes and qualified electronic time stamps for ensuring the accuracy of date and time of these documents. Notwithstanding,

---

52 B. Jérôme, Marianne Fraefel, and Reinhard Riedl, op. cit. 65.

53 Tsatsou Panayiota, Silvia Elaluf-Calderwood, and Jonathan Liebenau, op. cit. 305.

54 eid.as, op. cit. 1.

qualified electronic trust services are legally admissible as court evidence throughout the EU[55]. Use of these services provide the advantages of accurate date/time, verification and validation of identity, and detection of unauthorised modification for authenticity and integrity purposes[56].

[55] Katehakis, Dimitrios G., George Pangalos, and Andriana Prentza, op. cit. 22.

[56] eid.as, op. cit. 1.

2.8 Case studies of eIDAS implementation

The National Interoperability Framework Observatory (NIFO) publishes initiatives and policies regarding the implementation and delivery of electronic public services in EU countries. Sweden, Norway, Netherlands, and Ireland are some of the EU member states that have implemented eIDAS-compliant requirements in the recent past. For example, the Dutch Parliament (both Chambers) approved the eIDAS Act in December 2016. The Act establishes the procedures for implementing eIDAS into existing national laws. The Agency for Public Management and eGovernance (Difi) of Norway has set out a shared electronic signing service available to all public organisations. Similarly, in May 2016, the Swedish Parliament supported the process of implementing eIDAS as a supplementary law. In September 2016, the Irish Government opened the MyGovID – a shared online identity solution allowing secure access to diverse eGovernment services[57]. Therefore, EU member states are making major steps to ensure widespread adoption of secure and interoperable eIDs for their e-government services.

[57] ec.europa.eu, *eGovernment factsheets*, [website], 2017, https://ec.europa.eu/digital-single-market/en/news/egovernment-factsheets-2017, (accessed 18 October 2017).

2.9 Limitations of eIDAS

Despite the fact that eIDAS is intended to be technology neutral, some EU member states may impose specific hardware and software requirements. Consequently, unless comprehensive discussions are held by parties from different territories, interoperability issues are likely to emerge. Moreover, the security of eIDs, which is critical to trustworthy cross-border and cross-sector mutual recognition of eID means may be inhibited. Lack of adequate technical interoperability across the notified eIDs may challenge their security and trustworthiness levels. Moreover, some trust services may not be readable or verifiable because of technical issues lying beyond direct control of an entity required by eIDAS to recognise them. Here, the entity represents the addressee of a specific eIDAS obligation. To make matters worse, such an obligation does not require any public administration to implement the technical requirements appropriate for readability and verifiability of all trust services[58].

It is also not an obligation that member states communicate their national eIDs to the European Commission. Moreover, systems deployed by public authorities and businesses to control internal processes using trust services are not subject to eIDAS requirements. Therefore, the regulation covers only those trust services targeting the public with impacts on third parties. While these ensure that the commission does not interfere with eIDs and associated infrastructures deployed by member states, it attracts several concerns. For example, are all member state's eIDs recognised by the Commission from the context of interoperability? Moreover, how could member states learn the eIDs and related means used by others without a notification obligation? eIDAS attempts to address these 'open' issues by encouraging

---

[58] Katehakis, Dimitrios G., George Pangalos, and Andriana Prentza, op. cit. 26.

cooperation by every member state to ensure information sharing with the ultimate goal of ensuring mutual recognition[59]. Nevertheless, there still lacks an assurance that member states will cooperate.

While eIDAS require EU member states to include qualified TSPs and services in their national trusted lists, non-qualified electronic trust services may still be added in the lists provided they are explicitly marked as non-eIDAS compliant[60]. Consequently, EU citizens relying on non-qualified trust services may have the legal validity of their electronic signatures, electronic time stamps, and electronic seals among others challenged. For example, date certainty and the identity of signatory are common material concerns in law, especially in electronic contractual documents.

[59] Elizabeth, Kennedy, and Christopher Millard, op. cit. 98.

[60] ec.europa.eu, EU Trusted Lists, [website], 2017, https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers, (accessed 27 October 2017).

2.10 Gaps in existing literature

From the review of existing literature, it can be seen that online platforms come in many forms – from dissimilar corporate portals to social networking sites and payment gateways, and many others. These are applications that operate in diverse markets across the world, interconnecting organisations, and individuals. Moreover, the EU has focused on ways through which it can further grow its digital economy, particularly the eIDAS regulation that establishes a cross-border and cross-sector legal framework for electronic transactions, eID and trust services. However, eIDAS does not specify when one or more trust services are required for an electronic transaction or the type of service that is essential. Therefore, every EU member state is free to dictate the transaction instances when a specific trust service should be required. In addition, existing literature lacks a universal roadmap for implementing eIDAS requirements to cover the vast number of electronic transactions in the EU market. Therefore, it is worth investigating how eIDAS-specific trust services could be implemented in the Hellenic e-Government environment for an empowered digital economy in the country and the Europe at large especially in the considering aspects of security, trustworthiness, convenience, and interoperability?

3.0 Research Methodology

This research and its outcomes have been realised through desk research and in-depth review of books, journal articles, conference papers, technical sites, and various open documentary sources relevant to the research topic. Google search engine, ProQuest, EBSCOhost, Google Scholar, and Google Books were the major search tools used to discover documentary sources published. Only relevant sources published in English were used. Information relevant to the research topic was identified and collected as the researcher reviewed the selected materials. Thematic analysis was used to analyse the qualitative data that was collected from secondary sources. Key themes were identified and explored in a comprehensive manner.

Desk research and associated review of literature instead of carrying out an empirical study may attract researcher bias while extracting textual data from secondary sources[61]. However, multiple sources of secondary data were leveraged to bolster understanding into various issues and come up with clear implications and conclusions. Regardless of the obvious limitation of high likelihood of researcher bias, desk research is an approach that delivers huge volumes of secondary data without having to make resource-intensive fieldworks and actual collection and analysis of primary data[62].

---

[61] Chenail, Ronald, 'Interviewing the investigator: Strategies for addressing instrumentation and researcher bias concerns in qualitative research', *The Qualitative Report*, 16/1 (2011), 255-262.

[62] P. Shields and Nandhini Rangarajan, *A playbook for research methods: Integrating conceptual frameworks and project management* (New Forums Press, 2013).

The research project may be categorised as ‘no risk’ because it does not involve human participants. Therefore, no ethical measures were taken to ensure informed consent, anytime or voluntary withdrawal, and data and identity protection necessary to avoid potential confidentiality breaches.

4.0 Results and Discussion

4.1 Summary

The eIDAS Regulation took effect on 1st July 2016 and it establishes a solid legal framework for eID and electronic trust services related to electronic transactions. It applies to all member states of the EU, introducing mutual recognition of notified eIDs as well as electronic trust services like electronic signatures, website authentication, electronic time stamps, and electronic seals. With eIDAS, businesses and the public at large are allowed to use their individual eIDs to access resources, especially public services offered in other European countries. It creates an EU-wide market for the aforementioned electronic trust services by enabling cross-border technical functionality and legal admissibility and certainty just like paper-based identification schemes and processes. In this regard, the regulation ensures that public authorities, businesses, and citizens conducting online transactions in the Union are confident that their electronic signatures remain legally admissible across borders and sectors.

eID and electronic trust services have become core elements of the EU digital market as they provide well-known benefits, especially from the perspective of legal certainty as well as time and cost savings. With legally valid e-signatures, the trustworthiness of electronic transactions will be greatly enhanced, and the European digital economy is expected to grow sustainably. Indeed, this regulation is a pivotal milestone that provides a truly predictable legal and regulatory environment for government agencies, businesses, and citizens to securely and seamlessly access services and transact online. Regular compliance assessments based on eIDAS and national law requirements are necessary to guarantee strong eID and electronic trust services regarding a country. Moreover, such a move would go a long way in enabling secure,

trustworthy, and seamless cross-border and cross-sector electronic transactions that may eventually emerge as the natural approach to everyday interactions.

4.2 Theoretical implications

4.2.1 Mutually recognised eIDs

The European Commission divides the plan for eIDAS implementation into two main categories – eID and electronic trust services. The Commission called for collaboration on eID. Member states are required to cooperate and exchange necessary information to foster practical security, connectivity, and interoperability of their eIDs and eID means. Moreover, eIDAS provides the minimum technical requirements and procedures for low, substantial, and high assurance levels for eID means[63]. Member states may use the assurance levels as the benchmark for mapping and comparing their domestic eIDs and eID means against. Every EU member state is required to recognise all eID means issued in a different state and which has been communicated to the European Commission. The circumstances and means of notification are clearly defined by the Commission to facilitate automated processing and ease of use of eID means. This is mainly geared towards achieving mutual recognition and interoperability of cross-border and cross-sector eIDs and enabling EU citizens to carry out electronic interactions.

On the implementation of electronic trust services, eIDAS seeks to enhance transparency, security and trust, legal certainty, and interoperability in the EU market through EU trusted lists and technical neutrality. In this regard, the regulation requires qualified ETS providers and ETSs to be clearly differentiated from other providers and forms of trust services. This way, EU citizens can consciously and confidently take advantage of qualified ETSs to transact electronically. eID and trust services may soon become an everyday reality as EU citizens

---

63 eur-lex.europa.eu, op. cit. 1.

securely do all kinds of electronic/online transactions within a 'click' of the button[64]. Consequently, electronic transactions stand to become the most prevalent form of engagement and interaction for EU citizens[65].

[64] ec.europa.eu, *Back to the e-future: accelerating implementation and uptake of eID and trust services*, [website], 2015, https://ec.europa.eu/digital-single-market/en/blog/back-e-future-accelerating-implementation-and-uptake-eid-and-trust-services, (accessed 25 October 2017)

[65] ec.europa.eu, *Workshop: e-Signatures & e-Seals – Opportunities and Challenges*, [website], 2016, https://ec.europa.eu/digital-single-market/en/news/workshop-e-signatures-e-seals-opportunities-and-challenges, (accessed 28 October 2017).

4.2.2 Electronic trust services and cross-border legal validity

EU member states are obliged to create, publish, and maintain domestic trusted lists comprising the qualified TSPs as well as the qualified trust services they provide. The trusted lists are published and secured with suitable electronic signatures and electronic seals as member states notifies the Commission. They are then availed to EU citizens through a properly secured Web server[66]. Therefore, the 'qualified' status applies to all TSPs and ETSs published in these lists. Moreover, the EU trusted lists help build trust and ensure certainty among multiple market operators by indicating the statuses of providers and their services, while at the same time fostering greater interoperability of several qualified ETSs. Public administrators, businesses, and citizens are the major users of ETSs. They benefit from the predictable legal effect and trustworthiness related to specific qualified trust service providers and trust services that explicitly appear as 'qualified' in domestic trusted lists. Nevertheless, member states are free to introduce 'unqualified' trust services into their domestic trusted lists provided there is clear indication that they do not comply with eIDAS[67].

---

66 ec.europa.eu, EU Trusted Lists, op. cit. 1.

67 Ibid. 1.

4.2.3 Requirements for qualified trust service providers

The 'qualified' status for TSPs is granted by various EU member states' supervisory bodies. It is worth noting that each country in the Union has a supervisory body that assesses domestic TSPs prior to granting them the 'qualified' status. Qualified TSPs should ensure that they implement eID and trust services that comply with the eIDAS requirements as mandated by EU and national regulations. Furthermore, operators should put into consideration the cybersecurity risks (such as fraud and data breaches) associated with increased use of trust services[68]. The fact that eIDAS enables qualified electronic signatures, qualified electronic seals, qualified timestamps, and others basically ensures stronger legal implications. Such subsets of trust services allow particular legal premises since they are issued by qualified TSPs only.

[68] Elizabeth, Kennedy, and Christopher Millard, op. cit. 106.

4.3 Practical implications for the Hellenic e-Government environment

4.3.1 Major eIDAS principles

EU member states have already implemented eIDs based on disparate technologies such as smart cards and passwords; therefore, eIDAS does not require synchronisation of the eID means themselves. Instead, it opts for higher levels of interoperability between diverse national eIDs[69]. The principle of voluntary notification of domestic eIDs to the European Commission applies to all EU member states. However, the mutual recognition of all notified eIDs is mandatory[70]. Therefore, the two principles complement each other. As an EU member state, Greece is required to recognise eID means notified to the Commission by other nations for seamless and secure cross-border electronic authentication for its online services.

eIDAS mandates accountability or liability for fulfilment of an interoperable framework – technical interoperability among eIDs. At the same time, service providers have an obligation to protect data from security breaches that would inhibit the benefits of the much aspired prosperous EU digital economy. Therefore, concrete responsibility and trust is necessary throughout the entire eID and authentication process to ensure that personal identification data is confidential, authentic, and accurate at all times. At no point does the framework put the requirements on eIDs of a specific member state; it is a shared responsibility.

The eIDAS Regulation is mainly concerned with unique identification of persons – 'natural persons, legal persons (or businesses), and natural persons acting for legal persons'[71].

---

69 Bender, op. cit. 156.
70 Ibid., 156.
71 eur-lex.europa.eu, op. cit. 1.

Therefore, the regulation must define a universal minimum data set for each of these categories of entities requesting for services. However, member states are allowed to introduce additional attributes to the already defined minimum data set, while ensuring the uniqueness of identifiers. It is worth noting that eIDAS separates the concepts of eID and e-signature, where the former entails the identification of entities usually before the commencement of electronic transactions. The latter notion represents the conclusion of electronic transactions by electronically signing relevant electronic documents is a manner analogous and/or equivalent to a handwritten signature. The regulation however creates room for server-based and remote signatures as demonstrated in[72], enabling greater efficiency and flexibility potential in eID and e-signature markets.

[72] Bender, op. cit. 164.

4.3.2 Opportunities and limitations of eIDAS in relation to the Hellenic e-Government

Conventionally, EU member states have been independently establishing their national online services and eID means. Therefore, there were obvious challenges in harmonisation of eID and trust services in the EU because of differing technologies and security capabilities. Consequently, it was challenging to assure citizens of efficient and effective cross-border services due to security, transparency, reliability, and interoperability challenges that faced eID mechanisms. Luckily, eIDAS ensures that local administrators, businesses, and people can use their domestic eIDs to access cross-border public services.

The digital single market as a European Commission strategy creates invaluable opportunities for further enhancing market digitisation. It has the potential to support the creation of new business models with improved value propositions by unlocking underlying benefits to various EU member states and sectors[73]. eIDAS plays an integral role in the fulfilment of the objectives of the EU digital market as it offers a predictable legal framework for eID and electronic trust services. This way, EU public and private organisations as well as citizens are better placed to confidently embrace electronic transactions. Therefore, electronic trust services regulated by eIDAS are crucial to realisation of the goals of the digital single market strategy.

Effective and efficient e-government may deliver a wide range of benefits for government agencies, businesses and citizens, including greater levels of transparency and service delivery satisfaction. Other benefits include low-cost and quick processes. However, e-government

---

[73] P. Sachar, Pohlmann Norbert, and Reimer Helmut, *Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2003 Conference* (Springer Science & Business Media, 2004).

should not be mistaken with mere IT systems. Instead, it entails rethinking authorities and processes in addition to change of behaviour towards efficient delivery of services to people. With realisation of cross-border delivery of digital public services, people can move freely without any compromise to the efficiency and effectiveness of public services beyond their national boundaries. eIDAS creates a shared and interoperable legal framework that enable e-government capabilities[74].

The eIDAS principles of interoperability, mutual recognition, and notification may help protect existing domestic investments. Additionally, they ensure that countries can continue using their unique eIDs that fall beyond the competence of the EU regulatory framework. Therefore, Greece may maintain its current technologies and processes for eID and electronic trust services while making notifications to the Commission accordingly. However, these principles come with substantial risks. To start with, technical interoperability should be accompanied by high levels of security and privacy. In addition, relying parties must understand the security level of the mutually recognised eIDs in order to make more informed risk management decisions. Such information would help reject eIDs that are too weak to guarantee secure authentication for online services[75]. Therefore, authentication for Hellenic e-Government infrastructure would be based on absolute verification and verification of businesses and citizens. This way, the risk of unauthorised and illegal access to online services will be greatly

---

[74] ec.europa.eu, *eGovernment & Digital Public Services*, [website], 2016, https://ec.europa.eu/digital-single-market/en/policies/egovernment, (accessed 28 October 2017).

[75] K. Andrea and Francesconi Enrico, *Electronic Government and the Information Systems Perspective: 4th International Conference, EGOVIS 2015, Valencia, Spain, September 1-3, 2015, Proceedings* (Springer, 2015).

reduced. Issuing certificates for website authentication reassure users that online services are provided and managed by a trustworthy entity, thus promoting trustworthiness of content and services related to authenticated sites. Website authentication also ensures that the certified providers (in this case the Hellenic Government) are accountable for any security issues[76].

It can be argued that the regulation is typically a compromise as it is does not provide the details that would be of critical importance to technical personnel. For instance, material technical interoperability and security requirements are overlooked at the expense of legal and regulatory details that also tend to seem substantially sparse. Therefore, it may be challenging to assure harmonised eIDAS implementation across the EU unless necessary implementing acts are established in a timely manner. Moreover, the future may see considerable challenges in attempts to use the three primary assurance levels in creating a sustainable balance between cybersecurity and ease of use.

[76] ec.europa.eu, *eIDAS Stakeholder event: Workshop on Website Authentication – opportunities and challenges for the market*, [website], 2016, https://ec.europa.eu/digital-single-market/en/news/eidas-stakeholder-event-workshop-website-authentication-opportunities-and-challenges-market, (accessed 28 October 2017).

4.3.3 The roadmap for eIDAS implementation in the Hellenic e-Government environment

This study has demonstrated the current state of eID and electronic trust services as primary components of the eIDAS Regulation. In addition, the implications of eIDAS to EU member states have been explored. The eIDAS Regulation champions for use of mutually recognised eID and electronic trust services offered by qualified TSPs as a major step towards ensuring greater levels of cybersecurity, trust among parties, and legal certainty in relation to cross-border and cross-sector electronic transactions. The regulation covers the following major issues: eID, electronic documents, and electronic trust services[77]. Based on the findings, the www.ermis.gov.gr and www.gsis.gr portals appear to fit, as they are, into the eIDAS regulatory framework. What follows is a discussion of the management, policy and technological changes required for the Hellenic e-Government's eID and electronic trust services resulting from eIDAS.

Currently, the key enablers of e-Government in Greece are identified as eID, electronic documents (eDocuments), electronic safe (eSafe), authentic sources, and single sign on (SSO)[78]. From a technological perspective, Greece needs to create three assurance levels that help classify the notified eIDs based on their security. Classification should cover aspects of enrolment, issuance, and revocation of credentials. The 'low', 'substantial' and 'high' assurance levels are informed by initiatives and standards such as STORK QAA and ISO 29115[79]. As a best practice, the right mix of technical requirements should be pursued. This is because excessive

---

77 eur-lex.europa.eu, op. cit. 1.

78 joinup.ec.europa.eu, *eGovernment in Greece*, 2017, https://joinup.ec.europa.eu/sites/default/files/inline-files/eGovernment_in_Greece_March_2017_v2_00.pdf, (accessed 26 October 2017).

79 Bender, op. cit. 158.

concrete technical requirements would inhibit advancements and interoperability. On the contrary, many open requirements could get too flexible to assure a practical security level.

It should be noted that each eIDs has a set of security goals that the technical interoperability framework mandated by eIDAS must fulfil depending on the stakeholders' requirements and expectations. For example, service providers are obliged to uphold the integrity/authenticity and confidentiality of the personal identification data they handle. On the other hand, citizens expect the confidentiality of their personal identification data to be protected by operators as part of respect to their privacy[80]. Therefore, an outcome-based approach should be adopted where fulfilment of security goals should be prioritised instead of relying too much on technology. In fact, eIDAS calls for technical neutrality when it comes to eID and trust services in order to enhance technical interoperability.

Service providers established within Greece and offering different online services to administrations, businesses and citizens located internally and externally should create a unique interface with the national infrastructure or node operator/connector. In addition, they may interface with other connectors to enhance technical interoperability. The European Commission provides invaluable eID-related services that Greece should take advantage of. For example, the Commission offers software solutions for sample eID implementation and testing in addition to services such as conformance testing and training, technical specifications (like eIDAS SAML standard and eIDAS interoperability), and stakeholder management.

---

80 Ibid., 158.

The existing Hellenic www.ermis.gov.gr and www.gsis.gr should fully support the eIDAS technological requirements. Greek citizens should obtain valid credentials with registration strictly based on personal identification. The country should develop and apply emerging technological eIDs in its e-Government portals as part of complying with eIDAS.

As an EU member state, Greece has legal obligations of observing mutual recognition and liability of eID technical interoperability. Therefore, Greece should enhance its cooperation with other EU member states so as to enhance information sharing and harmonise its eIDs and electronic trust services with the ones notified by other states. It will also go a long way in facilitating technical interoperability with the EU-wide eIDAS eID environment. Stakeholders tasked with managing the Hellenic e-Government portals should focus on establishing concrete capabilities for notification of cybersecurity breaches. Moreover, attribute and identity providers ought to seek certifications such as the ISO/IEC 27001 while ensuring compliance with domestic legislation. They are also expected to execute organisational role of notification of eIDs and maintaining appropriate assurance levels based on the enrolment, eID, and authentication and control of electronic identities[81]. At minimum, the Hellenic e-Government portals should support cross-border use of eID for authentication across the existing online platforms. This will greatly improve the mobility of businesses and individuals in the EU. It is a best practice to support accountability with policy-based assessment and reporting.

From the perspective of policy, the Hellenic Government should formulate a set of eIDAS policy requirements that should domestic node operators, attribute/identity providers, and service

---

[81] P. Bart and Demosthenes Ikonomou, *Privacy Technologies and Policy: Second Annual Privacy Forum*, *APF 2014*, *Athens*, *Greece*, *May 20-21*, *2014*, *Proceedings* (Springer, 2014).

providers should comply. The policy requirements should be properly communicated to various stakeholders to ensure that they understand their specific roles and responsibilities, and that they act accordingly. This will help in successful implementation of the regulation in the e-Government portals.

4.4 Reflections

This dissertation has successfully fulfilled the research aim and associated objectives. It has critically evaluated potential opportunities and limitations of the eIDAS Regulation. Generally, the regulation establishes a predictable legal framework for eID and electronic trust services that are critical to secure, seamless, reliable, and trustworthy electronic transactions across the entire EU digital market. Through its principles of interoperability, mutual recognition, and notifications, eIDAS may help EU member states create compelling online services for consumption by local authorities, businesses, and citizens located in any European country. From the perspective of the Hellenic e-Government environment, the regulation may help the Greek Government offer better services to businesses and individuals in terms of reliability, trustworthiness, affordability, and security. Security and privacy are especially important as they enable protection of personal identification data as part of upholding citizens' fundamental privacy rights. However, eIDAS comes with a number of limitations, for example, some countries may impose prohibitive technical (hardware and software) requirements. Other limitations include lack of assured cooperation between member states. Apparently, eIDAS appears to be a compromise since it fails to provide fundamental details of crucial importance to technical personnel. Lastly, the study has proposed a set of technological as well as management policy changes needed to ensure successful compliance with eIDAS in the context of the Hellenic e-Government environment.

4.5 Future research considerations

The fact that desk research comes with the limitation of researcher bias may negatively affect the validity of study results. Original authors may also introduce bias in their work, and this may be detected during review. Consequently, generally, the study lacks sufficient practical orientation. As such, an empirical study on this area is necessary to justify and improve on the reliability of this research project's findings. This could include a mixed-research methodology where comprehensive statistical and qualitative data will be collected and analysed.

5.0 Conclusion and Recommendations

The eIDAS Regulation promises a future whereby EU-wide use of highly interoperable, secure, reliable, and trustworthy eID and electronic trust services like electronic signatures and electronic seals will be a reality. Public authorities, businesses and citizens will be allowed to confidently, conveniently, and safely access online services and carry out almost all transactions electronically and across national borders. Definitely, this will be done in just a single click of a button. Literature shows that the EU has managed to move rapidly towards making this a reality. This is especially backed by notifications of domestic eID means along with their recognition across borders. However, this will only be achieved if the public and private sectors work collaboratively to further improve the technical interoperability of eID and electronic trust services in the entire EU, while ensuring that the security of electronic/online transactions will be upheld at all times. Consequently, digital transformation will be greatly fostered across borders and sectors toward realising a digital single market with innovative and competitive services.

In the context of Hellenic e-Government environment, an authentication framework is necessary to enhance the process of verifying and validating claimed identities that actually exist. The framework would also help establish that an entity is the actual holder of a specific identity. Then, it would enable authenticated users to carry out the requested transaction(s) electronically. With eIDAS implementation, Greek businesses and citizens will be allowed to identify themselves using qualified digital certificates from any part of EU and transact electronically. Therefore, Hellenic policymakers should prioritise the initiative of implementing eIDAS requirements in its e-Government environment towards exploiting associated benefits.