A survey on server-based electronic identification and signature schemes to improve eIDAS: with a new proposal for Turkey

Ozgun Erdogan[1] and Nurdan Ayse Saran[2]

[1] Innova Information Technology Solutions, Ankara, Turkey
[2] Department of Computer Engineering, Cankaya University, Ankara, Turkey

ABSTRACT

The design, development, and implementation of e-Government applications aim to improve the quality of daily life and facilitate the mobility of citizens by reducing the constraints imposed by existing borders. This study examines previous research in the literature on electronic identification (eID) credentials technologies and the projects carried out in Europe. This study focuses especially on server-based e-signing methods. In the light of these reviews, the applicability of a server-based mobile electronic signature model without disrupting local initiatives has been examined as a case study. As an exemplary case, Turkey's eID structure is examined from a technical and legal perspective. When creating the proposed server-based eID model, it was especially inspired by Austria's server-based approach in use. In this process, the suitability of the existing structure with the server-based e-signing method was examined. In addition, some suggestions were made to eliminate the problems that may prevent the use of the proposed server-based e-signing method. This study revealed that a server-based electronic signature approach would develop a more user-friendly and flexible solution in identity management. It was concluded that using a server-based signature approach would help achieve international standards for cross-border online identification methods.

Subjects Cryptography, Security and Privacy
Keywords Server-based e-ID, Mobile signature, Server-based e-signatures, Turkish e-ID, eIDAS

Submitted 15 February 2021
Accepted 13 September 2021
Published 13 October 2021

Corresponding author
Nurdan Ayse Saran,
buz@cankaya.edu.tr

Academic editor
Donghyun Kim

Additional Information and Declarations can be found on page 19

DOI **10.7717/peerj-cs.734**

INTRODUCTION

Electronic identification (eID) is gaining more and more importance as our lives shift to today's digital realm. For a successful and efficient e-Government system, countries develop services so that citizens can process their requests without physically visiting public offices. It is essential in the globalizing world that electronic identity applications can be used in one country and between countries. Therefore, governments need to develop ways to integrate digital services. Significant progress has been made in this regard in Europe. Since 1999, digital services of EU member states have been developed on the basis of a common legal framework, Directive 1999/93/EC (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31999L0093, retrieved 24.05.2021). The current eIDAS Regulation (https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014.html), is a continuation of the old directive representing "electronic

How to cite this article Erdogan O, Saran NA. 2021. A survey on server-based electronic identification and signature schemes to improve eIDAS: with a new proposal for Turkey. **PeerJ Comput. Sci. 7:e734 DOI 10.7717/peerj-cs.734**

Identification, Authentication and Trust Services". This Directive regulates electronic identity and trust services for electronic transactions to develop the single digital market in the EU. Under eIDAS, citizens and businesses can use their local eID when accessing public services in the other EU Member States using electronic IDs. The Regulation also sets standards for electronic signatures, timestamps, electronic seals, and additional authentication proofs. In this way, cross-border mutual recognition of electronic identity within the European Union is ensured.

Qualified electronic signatures are required for safe and trouble-free electronic transactions between countries. This study examines identity registration and verification techniques, which will be the primary layer of e-government architectures that can work across countries. This review aims to identify the main issues and problems that should be considered while developing an internationally operable e-identity system. Today, an authentication approach based on smart cards distributed by certificate authorities is widely used in e-identity systems. However, this approach has many disadvantages, both in terms of usability and cost (see in "Usability"). In the literature, a server-based signature scheme, an alternative approach that eliminates the existing disadvantages and enables international interoperability, has been proposed (*Orthacker, Centner & Kittl, 2010*). In addition, server-based schemes can increase usability by eliminating the need for end-users to carry smart cards and the card's loss or theft. It can also support the collection of homogeneous data by avoiding the use of different typologies for the Member States at the European level, thereby increasing cross-border interoperability. In addition, essential security requirements have been established for all components and services to create qualified electronic signatures with eIDAS. Server-side solutions can address these requirements in server-based remote signing methodolgy, and security concerns can be avoided. One of the primary aims of this study is to demonstrate how an alternative server-based signature scheme can be used for eID environments without disrupting local initiatives (*Hühnlein et al., 2019*). In this process, as a case study, we examined how a server-based e-signature method can be integrated into existing e-signature applications in Turkey, whether it will facilitate e-signature processes, and its compatibility with existing systems. In this case study, we identify the necessary steps to integrate a server-based e-signature method into the existing infrastructure successfully. The results of this study can significantly increase the applications of server-based electronic signature schemes in different sectors (*Aciobanitei, Luculescu & Pura, 2020*; *Aciobanitei et al., 2020*), thus accelerating the realization of the technology-neutral eIDAS vision.

Survey methodology

In this study, we first present the current developments in eID technologies to reveal the barriers and technical difficulties that may arise in adapting eID technologies to national government systems using a deductive research approach (*Yin, 2009*). We then focus on server-based remote signing technology and present a general theoretical framework for the applicability of this technology through a case study.

When examining eID systems, social, economic, political, technical, and technological factors should be considered. However, the focus of attention in this study is technical and technological factors.

The World Bank[1] has grouped technologies used for identification and authentication into three broad categories: credentials (*e.g.*, cards, mobiles), authentication and trust frameworks, and analytics (risk assessments). Risk assessment is out of the scope of this paper.

Research Questions are as follows:

- What are the advantages and disadvantages of the current widely used Secure Signature Creation Devices (SSCDs)?
- Is it possible to reduce digital fragmentation and increase cross-border interoperability in the use of e-services by using remote signing with mobile solutions?
- Can remote signed eIDAS be implemented in Turkey without breaking the existing structure of local initiatives?

Search process

The study aims to review relevant research and the body of knowledge available to provide a holistic approach to research questions. All technical terms have been conveniently introduced and explained. While searching for relevant sources, a desk study (previous studies, reports, regulations, EU Commission's web pages, articles, etc.) has been conducted. In order to carry out this kind of research, we examined our search results in two dimensions; regulations and academic studies. The keywords "e-ID" and "e-IDAS regulation" for both "in Europe" and "in Turkey" has been searched in Google Scholar resulting in 177 articles. Also, the keywords "identity management" and "server-based signature" have been searched in Google Scholar resulting in 11 articles. The reviewed papers are mainly in English. The subject area covered is computer sciences. We excluded the articles that focus on cryptographic implementation techniques such as blockchain, pairing-based, and specific applications for universities, medical, financial. Also, we excluded the papers that focus on legislation, law, strategy, and justice. For the regulations, the search strings created to retrieve information from the site: ec.Europa.eu, site: www.resmigazete.gov.tr (for Turkish regulations) and also The Information and Communication Technologies Authority (ICTA) (Turkish: Bilgi Teknolojileri ve İletişim Kurumu (BTK)), General Directorate of Population and Citizenship Affairs (Turkish: Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü). Since we are focusing on the European eID system, we excluded the projects and regulations outside the European Union.

This study is intended for the benefit of government policymakers, other relevant public officials, as well as private sector partners and researchers. This article's primary purpose is to present the components of a common electronic identity approach regarding eIDAS regulations and reveal the current situation, especially in the Member states.

The article's organization is as follows: "Background" primarily discusses the main concerns of developing e-ID technologies. Next, we define the authentication factors, give

[1] Technology Landscape for Digital Identification, https://documents1.worldbank.org/curated/en/199411519691370495/Technology-Landscape-for-Digital-Identification.pdf, retrieved 23/05/2021.

the advantages/disadvantages of Secure Signature Generating Devices (SSCD) as a possession factor, and the features that a qualified electronic signature should provide. We also provide the security assurance level, technology, and standards that an SSCD must meet. In “E-ID in Europe” and “E-ID in Turkey”, we provide an overview of current relevant studies in Europe and present the current situation in Turkey. The proposed study reviews 20 papers that summarize country cases and four projects in Europe to answer the research questions. The following section presents the remote signing e-Identity System framework and the technical details required to implement it. Next, “Discussion” discusses the applicability of the method. Finally, “Conclusions” concludes the study.

BACKGROUND

This section focuses on the basic concepts of electronic identity, which form the basis of the study. First of all, the basic issues related to eID will be mentioned, then authentication factors, secure signature creation devices, qualified electronic signature, security assurance levels, and eID technologies and standards will be discussed, respectively.

Main issues in eID

There are many important issues related to electronic identification. Beyond privacy concerns, interoperability and usability must also be met by electronic identification in eIDAS. This section explains these important concepts.

Privacy

The Government-issued/recognized eID of a person contains mainly three parts;

- identification data such as a photo or biometric data
- possible user profile data such as citizenship
- authentication credentials such as digital certificate and the corresponding private key (for authentication and digital signing purposes)

The collection and processing of Personally Identifiable Information (PII) may bring privacy concerns (*Szadeczky, 2018*). Hence, it is necessary to associate the claimed identity with the applicant providing identity evidence for appropriate identity validation and verification. Therefore, it should be limited to the minimum required to validate the existence of the claimed identity. Also, it should prevent unauthorized access to the identity token (*Dumortier & Vandezande, 2012*; *Han, Chai & Liu, 2012*).

Usability

Usability of electronic identification is a challenging task since eIDAS promotes the seamless and widespread use of secure eID across the Member States. According to commission report[2], it should be useful, usable (easy to use), desirable (images and other design elements should be used to evoke emotion and appreciation), findable (content needs to be navigable and locatable onsite and offsite), credible (users must trust and believe what you tell them) (*Zefferer et al., 2014*).

[2] The user experience of eIDAS-based eID, https://ec.europa.eu/cefdigital/wiki/download/attachments/52600425/20190206_eID_Main_report.pdf?version=1&modificationDate=1551177429365&api=v2, retrieved 24.5.2021.

Interoperability

It is defined as “the ability of a system or a product to work with other systems or products without special effort on the part of the user, covering both the holder of the eID and the counterparty on the receiving end of electronic communication” (*Myhr, 2008*; *Mocanu et al., 2019*). Two main issues may be listed as cross-border operability and fragmentation.

- Cross Border Operability: A pan-European eID is closely connected with cross-border operability. It is defined as “a citizen from one country to have access to an application in another country” (*Leenes et al., 2009*). Due to the increasing mobility of citizens, citizen identification across borders is a major issue that needs a solution for maximizing the potential of cross-border service. Therefore, interoperability across the border of national electronic identity management systems (*Melin, Axelsson & Söderström, 2016*) becomes more and more important (*Sideridis et al., 2017*; *Sedek, Sulaiman & Omar, 2011*).
- Fragmentation: Fragmentation is also a common problem with identification systems. It separates identification structures to satisfy sector-specific demands without establishing standards (*Rivera, Milena & Kristjan, 2015*). The same basic information is collected from the users repeatedly and used for authentication purposes in separate databases of institutions such as government institutions, hospitals, telecommunication companies, and banks. As explained in the *FORMIT (2013)* Foundation’s e-Signature Final Study Report: “Existence of different typologies of e-signature has allowed the Member States to apply the Directive (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31999L0093) with certain degrees of freedom, generating more confusion than opportunities in cases that require interoperability across the national boundaries.” Adding different implementations and sector-based solutions to provide identity validation alternatives causes the overall system’s usability to get more complicated for the end-users.

Also, accountability, and transparency are fundamental issues in identity management systems (*Protopappas, Sideridis & Yialouris, 2020*).

Authentication factors

Authentication factors can be divided into three categories (*SecSign (2019)*):

- Knowledge-based factors (what-you-know)
- Possession-based factors (what-you-have)
- Inherent factors (what-you-are)

The authentication system may be either two-factor or three-factor depending on the number of parameters (*Patel et al., 2020*), and multi-server systems are preferable in eID technologies. At least two different authentication factors are mandatory for such a system (*Nikolouzou, 2020*). Biometrics are used as inherent factors. In recent years, multi-modal and behavioral biometrics have become more popular in terms of security. Since mobile devices can verify transactions using built-in sensors, multi-modal biometric authentication is also preferred. Various studies investigate the reliability and security of biometrics. The different factors should be chosen to counter different threats/attack vectors. But in this study, we focused on possession and knowledge, ignoring the third factor for simplicity.

Secure signature creation devices (SSCD)

A secure signature creation device (the synonymous "QSCD" under eIDAS) is software or hardware that has been configured to generate an electronic signature as defined in eIDAS. Along with the developments in two-factor authentication schemes, different e-ID credentials technologies have been proposed, such as identification *via* smart card methods, mobile methods, citizen card concepts, etc. These solutions' advantages and disadvantages are listed below.

- Smart Card Solutions: There are various types of smart cards; contact/contactless smart cards. They connect to a reader either by physical contact or remote short-range interfaces such as radio-frequency identification (RFID) or near-field communication (NFC). USB tokens can also be examined similar to smart cards.

  - **Advantages:** stability, low level of usability (*FORMIT, 2013*). Since being the first e-signature solution, it became a regular practice in time; people could not abandon their habit easily.
  - **Disadvantages:** the necessity for specialized data input devices in combination with the associated software and location dependency (*Rath et al., 2014*); lack of necessary infrastructure and applications, high cost of transition, and integration to electronic environments, low awareness/lack of awareness (*Kabasakal, 2007*). Another consideration is the risk of losing the token. Such solutions should technically assure that the data cannot be read from the card's chip.
  - Citizen Card Solutions

    –**Advantages:** adding more features such as e-signatures, containing fingerprint and biometric information of one (*Stipsits & Kammerstetter, 2015*).

    –**Disadvantages:** hardware dependency (using a national ID card from one EU Member State to another Member State is not possible yet (*Huhnlein et al., 2016*)).

European Committee for Standardization has an architecture for a European interoperable eID system within a Smart Card infrastructure, (https://joinup.ec.europa.eu/collection/european-committee-standardization-cen/solution/architecture-european-interoperable-eid-system-within-smart-card-infrastructure/about), retrived 24.05.2021. Notified schemes based on eID cards with LoA (See in Security Assurance) high in 2019 (Italy, Estonia, Spain, Croatia, Luxembourg, Belgium, Czech Republic, Latvia, Lithuania, Slovakia, Germany, Portugal)[3].

- Mobile Solutions: Mobile technologies have various international standards for secure crypto applications such as OTP (One Time Pad), Mobile Connect (an initiative

[3] Overview of Pre-Notified and Notified eID schemes under eIDAS, https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS, retrieved 24.05.2021.

from the GSMA that aims to provide new digital authentication standards)[4]. Besides these, trusted hardware devices enable secure storage and isolated processing of sensitive data. Such as TPM (Trusted Platform Module by the Trusted Computing Group), ARM TrustZone, Trusted Execution Environment (TEE), and electronic chips called Secure Elements (*e.g.*, UICC (Universal Integrated Circuit Card), also known as Cryptographic SIM, NFC secure elements) (*Nyman, Ekberg & Asokan, 2014*).

- **Advantages:** ease of use; low cost to the user, and the possibility of signing independent of time and space.
- **Disadvantages:** the dependence on specific use cases (*Rath et al., 2014*), security (according to *Ruiz-Martnez et al. (2007)*) "mobile handsets" have reached a significant penetration rate in many countries such as Luxembourg (164%), Italy (128%), Hong Kong (117%), Spain (109%), Chile (74%), Argentina (64%), and so on. Also, the risk of malware exposure is a problem since cryptographic operations, and private data are contained in SIM cards (*Rath et al., 2014*).

Countries Austria, Belgium, Estonia, Finland, Germany, Iceland, Latvia, Lithuania, Norway, and Sweden, have completed their studies and launched their mobile eIDs (*Sagıroglu, Kabasal & Alkan, 2008*). According to *Leitold & Konrad (2019)*, mobile signature exceeds smart-cards by far. Increasingly, mobile phones are a platform for fingerprint, voice, and facial recognition. Therefore, using mobile phones in place of dedicated hardware may be a more affordable way to bring biometric authentication.

- Server-Based Solutions: In contrast to other solutions, in server-based solutions, the SSCDs are not under the physical control of the user. It is centrally implemented and shared among all users.
  - **Advantages:** eliminates hardware dependency (since no reader or additional software is required from the end-users side), cost-effective for large-scale deployments, user-friendly, and flexible solution (*Orthacker, Centner & Kittl, 2010*). There is no need for dedicated signing hardware on the user side. Also, it may be seamlessly integrated with mobile devices, web browsers, or client-side applications.
  - **Disadvantages:** most of the server-based approaches are tailored to specific use cases (*Rath et al., 2014*). User and server authentication are required. Most of them use SMS functionality while signatory proves his/her identity to the server, but not bound to SIM card or mobile network operator.

The usage of HSM (hardware security module) devices increases the security level (*Orthacker, Centner & Kittl, 2010*). It offers central management of eID services with proper standards, the integration of these separate services is provided at a sufficient level (*Rath et al., 2014*).

Qualified electronic signatures (QES)

With the introduction of Directive 1999/93/EC (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex\%3A31999L0093) that is Community Framework for Electronic

[4] Mobile Connect, https://www.gsma.com/identity/mobile-connect, retrieved 24.05.2021.

Signatures prepared by the European Commission, e-signatures that meet certain conditions became legally equivalent to the wet signatures. Therefore, QES needs to fulfill several requirements and be created in an SSCD based on a qualified certificate. According to Directive, an advanced electronic signature is a signature that is

- uniquely linked to the signatory
- capable of identifying the signatory
- created using means that the signatory can maintain under his sole control
- linked to the data to which it relates in such a manner that any subsequent change of the data is detectable

According to Directive, a qualified electronic signature is a signature that is

- based on a qualified certificate (specified in Annex I of the Directive)
- created by a secure signature creation device that needs to comply with Qualified Certificates requirement.

In practice, the underlying technology is based on public key infrastructure (PKI). We want to draw reader's attention that according to eIDAS, QSCD (Qualified Signature Creation Device) has to be operated by a QTSP (Qualified Trust Service Provider)[5].

Security assurance levels

While assessing an authentication mechanism, the threats that should be taken into account are online guessing, offline guessing, credential duplication, phishing, eavesdropping, replay attacks, session hijacking, man-in-the-middle, credential thefts, spoofing, and masquerading in the ISO 29115[6].

The STORK[7] project has created four Quality Authentication Assurance (QAA) levels. Level 4 is the most reliable, and level 1 is the least reliable. Currently, three levels of assurance (LoA) are accepted as high, substantial, and low, based on ISO 29115, STORK [STORK-D2.3], NIST [NIST-800-63-2] and CIR 2015/1502[8].

Technologies and standards in eID

There are many technologies and standards related to eID. In this part, first, the most widely used technologies are listed. Then, the most widely used standards and frameworks are presented.

- For secure information exchange-SAML (Security Assertion Markup Language-single sign on communication)
- For endpoint security-TLS (Transport Layer Security—a cryptographic protocol that provides communication security over a computer network)
- For identity authentication systems on mobile devices and web applications-FIDO UAF (Fast Identity Online Universal Authentication Factor), FIDO U2F (Universal 2nd Factor)[9]
- For delegating access-oAuth

[5] Conformity Assessment of Qualified Trust Service Providers, https://www.enisa.europa.eu/publications/assessment-of-qualified-trust-service-providers.

[6] ISO/IEC 29115:2013–Entity authentication assurance framework for additional information, Section 2.1.2.2.

[7] STORK, pan-European electronic-identity authentication project, https://ec.europa.eu/digital-single-market/en/content/stork-take-your-e-identity-you-everywhere-eu.

[8] Commission implementing Regulation (EU) 2015/1502 of 8 September 2015 on the minimum technical specifications and procedures for assurance levels for electronic identification.

[9] Note that FIDO U2F is developed in FIDO2 project; WebAuthn (Web Authentication; on device authenticator, web authentication and through browser) and CTAP(Client to Authenticator Protocol) are the primary outputs; CTAP is a user-controlled cryptographic authenticator (such as a smartphone or a hardware security key).

- For extra identity layer built on top of OAuth-OpenID connect
- For advanced electronic signatures formats[10],-XAdES[11], CAdES[12], PAdES[13] or ASiC ETSI Plugtests Baseline Profile[14].

Standards and Frameworks: Standardization is a critical issue to achieve the reduction of dependence on external suppliers, to prevent abuse of dominant market positions, to assure transparency, security and interoperability (*Blind & Gauch, 2009*; *Werle & Iversen, 2006*; *Sealed & Piper, 2007*). The whole list of standards for eIDs and TSPs are listed in Enisa Report ”Standardisation in the field of Electronic Identities and Trust Service Providers”[15]. The most widely used standards and frameworks are listed below:

- ISO/IEC 29003:2018—Identity proofing
- ISO/IEC 29115:2013—Entity authentication assurance framework
- NIST SP 800-63—Digital Identity Guidelines
- CEN/TR 419010—Framework for standardization of signature
- PKI Standards-X.509 (ITU) for the certificate format, PKIX (IETF) standards for core PKI and PKCS standards for interfacing to secure devices
- CEN 419241-Trustworthy Systems Supporting Server Signing.

E-ID IN EUROPE

In the beginning, countries formed their country-based solutions in order to get the most benefit from electronic signatures. After 2007, pilot projects like STORK1.5 (Secure Identity Across Borders Linked) (*Leitold, 2011*), STORK 2.0, and e-SENS[16] were started by EU organizations to support the cross-border identity validation (*Eichholtzer, 2009*). STORK is a Large Scale Pilot project that gathers 58 organizations from 19 Member States (*Leitold & Posch, 2012*). e-SENS was launched in 2013 gathers 100 organizations from 22 countries. As the eIDAS regulation (https://ec.europa.eu/futurium/en/content/eidas-regulationregulation-eu-ndeg9102014) introduced electronic identity and trust services for international electronic transaction schemes in 2014, researchers once again gave some thought to a global eID concept. A global project named FutureTrust[17] continues addressing a more straightforward and international way of online identification scheme (*Huhnlein et al., 2016*). e-Authentication (e-AU), e-Signature (e-SIGN), and e-Identification (e-ID) are used for handling governmental and administrative official procedures or services. Beyond these global projects, several projects have been conducted in Member States that reference architecture for the remote provision of eIDAS-related services such as SkIDentity[18] and FutureID[19] (*Hühnlein, 2014*). Another project, named Eksistenz, deals with security concerns such as ID theft (*Liu-Jimenez et al., 2015*).

[10] Note that although CEF (Connecting Europe Facility) supports the ETSI EN 319 xxx standards released in 2016, please note that Decision 2015/1506/EU still refers to the previous set of standards.

[11] XML Advanced Electronic Signatures (XAdES) Baseline Profile-ETSI, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eSignature+standards#eSignaturestandards-XAdES(XMLAdvancedElectronicSignatures)BaselineProfile.

[12] CMS Advanced Electronic Signatures Baseline Profile, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Standards+and+specifications.

[13] PDF Advanced Electronic Signature Baseline Profile, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Standards+and+specifications.

[14] Associated Signature Container Baseline Profile, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Standards+and+specifications.

[15] Standardisation in the field of Electronic Identities and Trust Service Providers, https://www.enisa.europa.eu/publications/standards-eidas.

[16] e-SENS, http://www.esens.eu/, retrieved 24.05.2021.

[17] FutureTrust, https://cordis.europa.eu/project/id/700542, retrieved 24.05.2021.

[18] SkIDentity, retrieved July 2021, https://www.skidentity.de/.

[19] FutureID, retrieved July 2021, https://cordis.europa.eu/project/id/318424.

As the technology of e-signatures continues to improve, countries continue to try to adapt their identity structures to the new advanced identity validation methods to achieve a more secure and usable work environment. However, with the different e-signature solutions used in other sectors, sector-based solutions and use cases are formed. According to the *FORMIT (2013)* Foundation's report, the member states have announced plans for a more open, accessible, and transparent administration using the latest electronic signature technologies. Throughout implementing the latest technologies, different typologies like server-based e-signature technologies are formed in order to provide a solution for these problems. The advantages and disadvantages of the latest technologies have been given in the preceding section.

Finland was the first country to issue a national eID card in 1999 (*Rissanen, 2010*). However, many countries have adopted national ID Card based identification and authentication methods over the past decades, including EU member states Belgium, Estonia, Austria, Sweden (*Göransson, 2018*), Italy, Spain (*Gómez de la Cruz, 2005*), Portugal, and Germany, etc. (*Roßnagel et al., 2012*). Estonia used the first national ID card with digital signatures in October 2002 (*Rivera, Milena & Kristjan, 2015*). Estonia also constitutes an excellent example with its successful integration system that connects the population register records with eID systems (*Rivera, Milena & Kristjan, 2015*). Although the id card-based method is the direction most countries seem to follow, it is still not possible in practice to use a national ID card from one EU Member State to another Member State just yet (*Huhnlein et al., 2016*). In addition to the classic national eID card solutions, member states have also notified schemes based on mobile solutions such as Estonian *Mobiil-ID*, the Latvian *eParaksts*, the Portuguese *Chave Móvel Digital*,the Belgian *FAS/itsmee* (*Mariën & Van Audenhove, 2010*; *Soyez, 2019*), the Danish *NemID* (*Nikolouzou, 2020*), the Moldavian (*Rosca, 2017*). However, it brings a high and increasing mobile penetration in Europe (85% in 2017 and estimated to go up to 88% in 2025) (*GSMA, 2018*). However, Estonia's and Austrian e-identity schemes (*Stranacher et al., 2013*) may be good examples of handling mobility problems (*Kubach et al., 2015*). In Estonia, the e-residency program developed an integration model ensuring the development of a unified system. The Austrian government first introduced the national card concept then improved their system towards server-based mobile eID strategies supporting cross-border identification of users (*Paulin, 2012*; *Aichholzer & Strauß, 2010*; *Behrens, 2012*; *Strauß & Aichholzer, 2010*). Austrian and Estonian e-government systems also constitute a base for cross-border identification of citizens. Server-based identity and signature solutions have recently gained popularity in recent years (*Rath et al., 2015*; *Lenz, Stranacher & Zefferer, 2013*; *Zefferer, 2014*; *Kubach et al., 2015*).

E-ID IN TURKEY

During the ongoing process of national citizen cards and studies towards the new e-signature law in 2019, the necessary steps to achieve a more practical and international online identification method are investigated in this study. In order to provide more user-friendly identity validation for Turkish citizens, the private sector and the Turkish government are continuously trying to adapt to the new solutions of identity validation arising from different technological developments. While these new technologies are implemented in the existing system over the years, different typologies of these solutions are formed, sector-based solutions are developed, and general concepts of cross-border operability and usability are overlooked. One of the main reasons for these heterogeneous implementation styles is the lack of clarity in implementation in Directive 1999/93/EC (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex\%3A31999L0093), the community framework for electronic signatures prepared by the European Parliament. In Turkey, different applications using different e-signature technologies results in different passwords for a single user. It raises a usability problem since individuals have to remember different passwords for various online services every day. For example, some governmental services require smart card-based e-signatures, such as e-prescriptions services used by doctors in the health sector. Simultaneously, people also need to have national ID cards to identify themselves officially, which is also capable of e-signatures. In addition to that, to handle their financial transactions, Turkish users have different passwords for each legal bank account they own because their bank may not provide an electronic signature login option. As a result, people are obliged to manage all these different passwords and identification documents in their daily lives.

Besides usability and fragmentation problems Turkish users face, the existence of different e-signature technologies results in other technical structures (*Zhang & Xiao, 2020*; *Wang et al., 2019*) that needed to be combined to establish a Turkish eID environment capable of cross-border validation. This non-standard and separate big data not only affects the citizens and also brings forth vulnerability problems for organizations to think about, such as struggling to manage the sheer volume of vulnerabilities (*Tang, Alazab & Luo, 2017*; *Dzikrullah & Rinjani, 2017*). The main limitations in these services are technical operability, cross-border interoperability, usability, and lack of legal harmonization. In the meantime, in Turkey, Electronic Signature Law No. 5,070 imposed in 2004[20] is still in force. Besides the national ID card system, dongle-based methods, SIM card-based methods, and recently oAuth methods are still used to authenticate users in Turkey's different platforms. On the other hand, despite the eIDAS Regulation effective from 2016, there has been no change in Turkey's e-signature law yet to comply with the eIDAS Regulation.

After the preparations of an electronic signature, law No. 5,070 in Turkey; electronic signatures have started to be used since 2004. After that, developments in e-government applications have also accelerated. For example, Turkey's e-government project, which aims to provide joint public services from a single point, became operational in 2008 with 22 services (*Information Society Statistics, 2011*). Since January 2017, applications have reached 3,027 services (*ITU, 2016*). Mobile electronic signature infrastructure was put into practice with telecommunication companies in 2007[21]. Today, three leading telecommunication companies serve mobile e-signatures in collaboration with six electronic signature certification authorities. According to the Turkish Electronic Communication Sector/Quarterly Market Data report of the Information and Communication Technologies Authority, the percentage of mobile signatures produced over electronic signatures in Turkey is only 14%, until the year 2019 (*Quarterly Market*

[20] Electronic Signature Law No.5070, https://www.resmigazete.gov.tr/eskiler/2004/01/20040123.htm, retrieved 25.05.2021.

[21] Regulation on the Procedures and Principles Regarding the Application of Electronic Signature Law, https://www.resmigazete.gov.tr/eskiler/2005/01/20050106-15.htm.

Data Report, 2019). Turkey's citizen card studies started in 2008 with the Scientific and Technological Research Council of Turkey (TUBITAK-UEKAE) (*Mutlugün & Adalier, 2009*). Citizen cards officially started to be distributed to citizens all over the country through the general directorate of population and citizenship affairs at the beginning of 2017. According to the public employees' e-population union[22], the number of distributed citizenship cards reached 37 million (almost half of the 82 million in Turkey) in 2019. Along with these solutions, Turkey also participated in some international projects initiated among European countries. Although different organizations from the EU carry out these projects, their joint mission was developing typical specifications for secure and mutual recognition of national electronic identities between countries. Other sectors adopting various methods increase the available system's complexity in implementing other e-signature solutions. Besides that, these new technologies' requirements can ensue as software or hardware requirements, which hardens eID providers' and individual's adaption processes. The need for a simple and inclusive identity authentication method arises day by day under these circumstances in Turkey. Therefore, providing architecture with higher usability and possibly an international solution for identity authentication is aimed at this study.

A SERVER-BASED ELECTRONIC IDENTIFICATION AND SIGNATURE SCHEME

A design of a server-based signature scheme should consider two essential steps to protect signature creation data; a robust authentication mechanism and the protection of the authentication data during communication between the user and the interface for server signature creation device (*Orthacker, Centner & Kittl, 2010*). In different schemes, the signature activation mechanisms and the approaches to ensure the sole control requirement vary greatly (*Leitold & Konrad, 2019*). In our scheme, as in the Australian scheme, a mobile phone (without any cryptographic module) is required as possession of the user. Only an OTP connection is sufficient instead of employing hardware secure elements. In the following subsections, a scenario to integrate remote signing strategy into the existing system in Turkey has been given; firstly, requirements are listed, then the four phases of the identity life-cycle are examined.

Recently, server-based approaches are becoming more common across countries. The difference is mainly on the level of the identity proofing and verification phase. In the proposed system, the server-based method relies on the concept that cryptographic operations are handled in hardware security modules (HSM) instead of users' local devices such as SIM cards or smart cards. Mobile phone identity proofing is done; however, the smartphone is not necessary; only OTPs are used. With the server-based signing, signing keys are held on a service provider's HSM (*Orthacker, Centner & Kittl, 2010*). With this approach, the need for users to handle their own private keys is eliminated. Austria is one of the exemplary countries where the server-based eID concept is implemented and used for several years countrywide (*Orthacker, Centner & Kittl, 2010*; *Stranacher et al., 2013*). They have made the necessary legal arrangements in its electronic signature law allowing the usage of server-based methods in the country in

[22] TC Icisleri Bakanligi-Nufus ve Vantandaslik Genel Mudurlugu-TC Kimlik Karti, https://www.nvi.gov.tr/tc-kimlik-karti.

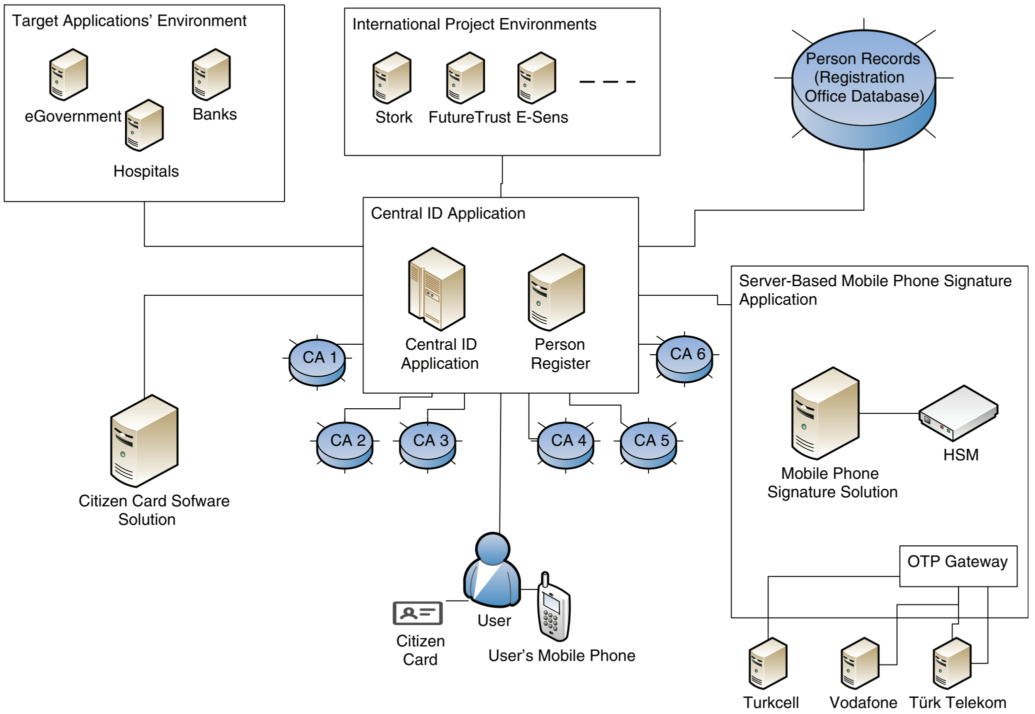
Target Applications' Environment
eGovernment
Banks
Hospitals
International Project Environments
Stork
FutureTrust
E-Sens
Person Records (Registration Office Database)
Central ID Application
Central ID Application
Person Register
Server-Based Mobile Phone Signature Application
CA 1
CA 2
CA 3
CA 4
CA 5
CA 6
Mobile Phone Signature Solution
HSM
Citizen Card Sofware Solution
OTP Gateway
User
Citizen Card
User's Mobile Phone
Turkcell
Vodafone
Türk Telekom

Figure 1 **eID infrastructure.** Full-size DOI: 10.7717/peerj-cs.734/fig-1

addition to the leading national ID card solution (*Orthacker, Centner & Kittl, 2010*). In Turkey, there has been no attempt to implement any national server-based eID structure so far. A server-based eID approach is adopted for interoperability and also to increase usability. Despite differences, the modular and flexible solution of *Rath et al. (2014)* eases the implementation of the method and helps us establish a preliminary eID infrastructure for Turkey.

In this part, requirement analysis is conducted, and primary necessities of the Turkish eID scheme are specified as below;

- A central ID application in eID structure that provides an integration of Citizen Card Software's systems, General Directorate of Population and Citizenship Affairs's system, and e-signature data kept on certification authorities (CA) is given as in Fig. 1.

  –It should support both citizen card signatures and server-based signatures.

  –The application should manage a common infrastructure between certification authorities, General Directorate of Population and Citizenship Affairs securely.

  –It should include a person register component, and it should support the registration types; face-to-face registration, self-registration (using existing qualified eIDs), and registration *via* trusted organizations (such as a bank or a university).

  –Person register application should serve as a common point of contact enabling all outside ID sources to connect with it. It should provide a standardized ID infrastructure.

- A server-based signature application that is capable of creating server-based e-signatures in a HSM device is necessary, as in Fig. 1.

  –HSM usage in the server-based signature solution is needed to improve the security level.

  –Web interfaces (usage) are necessary to render the server-based signature usage.

Enrollment phase

The enrollment phase is the first phase of an eID scheme; the user has two options to register; use an existing eID or apply for a new eID (providing his/her legal identification document).

- **Application *via* new eID and Registration:** The user applies registration authority with his/her breeder document such as an official ID, a passport, or a driving license. The registration officer (National Identity Provider) conducts face-to-face validation/verification of the user. Officer manually registers the user in the person register system with the user's specific data (*e.g*., name, national identification number, phone number, etc.) *via* a web-based form. A one-time code is sent to the user's provided mobile phone number for validation. If the user's one-time code is valid, a unique identification record and an activation code have been created in the person register application.
- **Registration *via* Existing eID:** If the user wants to use his/her existing eID information stored in his/her national ID card, firstly, he/she connects his/her ID card to a card reader. Then he opens an online person register application provided by the central ID application component, an online environment verifying the user's identity and enabling users to complete the registration on their own. The user creates a unique identification record in the person register application *via* a web-based form. The user's existing eID is validated through this web service and the user's certification authority. If the existing eID is valid, a one-time code is sent to the user's provided mobile phone number for validation. If the user's one-time code is valid, a unique identification record and an activation code have been created in the person register application.

Created identification record and activation code are shared with the server-based mobile phone signature application so that the user can log in to the proposed server-based mobile phone signature application with his/her phone number and activation code. Also, an activation code is sent to the user's mobile phone.

Identity proofing and verification phase

After a successful login to the server-based e-signature application, the user can start the signature creation process. A unique identification record is already shared with the server-based e-signature application, and there is no eID or signature created up to this point. The user fills an activation form and determines a unique secret password (with a revocation PWD) to create an eID for himself/herself with the help of a CA. If the user already has an existing eID (Registration Alternative 2), he/she does not need to choose a certification authority. If the user does not have a current eID (Registration Alternative 1), he/she selects a certification authority in the activation form. The user is directed to the chosen certification authority's payment system to complete the necessary payments. In the current situation, CAs in Turkey produce certificate and revocation status records and sign them with their own signature creation data. They are also responsible for the distribution, renewal, and disclosure of revoked certificates to all parties. In our proposed scheme, they are responsible for the same tasks, but they don't give the users' key pairs in a dongle or smart card; they share the information with the central eID application.

After the activation form is completed, a one-time password (OTP) is sent to the user's provided mobile phone number for validation. If the user's one-time code is correct, a signing key-pair generated in the HSM and an encryption key pair for the user are created in the server-based application's server with CA interaction. Note that, in this scenario, encryption and signing key pair are not the same. After an eID is created for the user, it contains a specific phone number and secret password information (plus revocation password) besides the user's personal information transferred from the person register. At the end of the process, created eID and keys are encrypted; the user's private signing key is stored in the HSM Module (encrypted with HSM's master key). The user's private key is encrypted using symmetric encryption with the hash of the user's secret password. All encrypted entities are stored under the server-based application securely.

The encryption keys are stored encrypted in the application server using the password of the user and the signatory's mobile phone number. A secret password has been chosen by the user while creating eID and it is stored in the system by hashing. By the way, HSM can only decrypt if the user is authenticated. Therefore sole control is on the user. The HSM initiates a qualified electronic signature by creating a challenge and a verification code, both to be delivered to the signatory's mobile phone.

Issuance (credential management)

In this phase, creating and distributing credentials are regulated; however, there are no physical credentials to develop/distribute in such a system. It uses the credentials already distributed. The maintenance of HSMs is central. The revocation should be legally regulated, CAs should publish revoked certificates.

Identity authentication

If a user wants to sign a document using an electronic signature, he/she may sign with server-based or national card-based authentication. If server-based signing is chosen by the user, in the web interface of the server-based e-signature application, the user is asked to provide his/her phone number and the secret password. Phone numbers and secret passwords are sent to the server-based e-signature application server *via* a secure connection. If the given information corresponds to an eID record in the system, the user receives an OTP to his/her registered mobile phone. After that, the user is required to provide the correct OTP in the web interface. During this process, a unique reference value is also created. This value is shown to the user in both the web interface and in the

SMS message. This reference value is used to prevent man-in-the-middle attacks and to ensure perfect forward secrecy[23]. After all of the provided information is verified within the system. Then, the electronic signature is performed on behalf of the user inside the HSM module. Then signed data is transferred to the target application through the central ID application. After this phase, authorization and identity management is the ongoing process of retrieving, updating, and deleting identity attributes and policies governing users' access to information and services.

DISCUSSION

Technical applicability

The following technical factors should be considered to evaluate the method's availability in Turkey. Since 2017, Turkey has distributed about 37 Million Citizen cards with e-signature functionality to its citizens (*General Directorate of Population and Citizenship Affairs of Turkey, 2019*). The proposed solution combines the citizen card concept and the server-based mobile phone signature concept. Therefore, it is technically not difficult to implement this method as there is no need to change the existing infrastructure.

According to the *FORMIT (2013)* foundation's study report prepared by the European Commission in 2013, in the matter of e-signature products, three factors; "usability", "security", and "interoperability" need to be taken into account and harmonized in order to find the optimal point of balance. Therefore, the proposed system's main contributions for Turkey's electronic signature scheme are usability increase and cross-border interoperability (model is applicable to Pan European Proxy Service (PEPS) model (*Lenz & Zwattendorfer, 2016*)), besides a sufficient level of security increase accordingly.

Usability

A centralized e-identity management technology enabling single eID for multiple services may free people from the burden of creating different accounts and managing multiple passwords for services (*Ruica, Pura & Aciobanitei, 2020*). Since no reader or additional software is required of users, a server-based signature is a comparatively cheap, user-friendly, and flexible solution. The mobile devices do not need special-purpose hardware (such as smart-card readers or Trusted Platform Module chips) and special-purpose SIM cards. The proposed solution can be implemented with non-smartphones as well. This convenience improves usability by extending the sphere of influence.

Cross-Border Functionality

The solution provides self-registration functionality where identification attributes can be read directly from the foreign ID card with a qualified certificate, allowing cross-border authentication (*Stranacher et al., 2013*; *Rath et al., 2014*). Central ID management prevents different levels of information in different systems at a national level. It supports the collection of homogeneous data for the Member States at the European level. With the introduction of eIDAS Regulation replacing the old eSignature Directive 1999/93/EC (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex\%3A31999L0093, retrieved 24.05.2021), across Europe, adopting the server-based eID methodology provides a

[23] Guidance for the application of the levels of assurance which support the eIDAS Regulation, https://ec.europa.eu > download > attachments.

legal structure for Turkey's e-signatures, and international eID schemes would be described and supported.

Security

According to *Sullivan (2018)*, the digital identity concept is supported not only for cost and efficiency purposes but also to reduce fraud. Different eID solutions are applied by various sectors such as banks, trading sites (shares, stocks), ticket sales (hotels, airplanes), shopping sites, the health sector, and government institutions in Turkey. This situation causes different security levels for other applications. A hardware security module (HSM) is a physical computing device that contains one or more secure cryptoprocessor chips. The server-based concept relies on HSM modules instead of SIM cards or smart cards to guarantee the security of the cryptographic operations (*Orthacker, Centner & Kittl, 2010*). With the remote signing, signing keys are held on a service provider's HSM. Therefore the need for users to handle their own private signing keys is eliminated. On the other hand, typical attacks on possession-based authentication factors are theft, duplication, or tampering; however, a server-based system against such attacks is indisputable.

Accessibility

Besides used technology, technical background for exceptional cases is also an essential aspect of the eID issue. In the event of losing or forgetting the actual secret password, the user can demand to change his/her password through a revocation password in the presented solution. Suppose the revocation password is forgotten or lost too. In that case, the person must pay a visit to the registration authority with an identification document to authenticate face to face.

In Turkey, disabled people are provided with their identification documents, but they may not perform legal processes due to their limitations. In that case, their legal guardians perform their necessary operations on behalf of them. Disabled people can still register the application and create a unique identification record for themselves, but they can not apply e-signatures. If a signature is needed for application, their legal guardian's signature is necessary. Today in Turkey, underage people (age of eighteen) have their identification documents for themselves; however, they can not legally provide e-signatures.

Legal applicability

Although the old Directive (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex\%3A31999L0093, retrieved 24.05.2021), does not comply with remote electronic signatures, the eIDAS Regulation (https://ec.europa.eu/futurium/en/content/eidas-regulation regulation-eu-ndeg9102014), also endorses this. eIDAS aims to reduce bureaucracy, make processes less costly, and make individuals' and companies' lives easier. For these purposes, eIDAS gives countenance to the use of server-based e-signing services to manage private keys on behalf of the users (*eIDAS, 2009*; *Polanski, 2015*). Since there is already a need for a structure compatible with eIDAS, the proposed design is a good solution to handling legal and technical obstacles. The fact that Austria's technical infrastructure (server-based e-signatures using HSM) is now considered a reliable and valid system according to eIDAS (2009) supports the applicability of the proposed solution for Turkey (Polanski (2015)).

As of the date of its entry into force, the eIDAS Regulation revokes the EU Directive 1999/93/EC (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31999L0093, retrieved 24.05.2021), which is the basis of the legal and technical framework of electronic signatures in Turkey. In this context, the "Report on the Regulation of Trust Services" was prepared by the Information Technologies Department of Turkey in 2018 (Activity Report 2018, 2018). Within the scope of harmonizing Turkey's laws with EU legislation, updates on trust services in Turkey's laws in line with eIDAS must be completed.

Besides these, the proposed server-based eID infrastructure is a product of a public-private partnership in Austria (EGIZ, 2009). Polanski's study mentioned that, the unification of e-trust services requires adoption and cooperation between states and private parties rather than complicated implementations (Polanski, 2015). Public-private partnership projects should be initiated to combine public and private sectors and create a homogeneous structure throughout the country. These projects should be managed and audited by the government. Governmental management of such projects is essential. However, the legal framework is constituted in a timely manner, the use of e-signature may not reach the expected levels due to insecurity in new technologies (Kabasakal, 2007).

CONCLUSIONS

In this study, we examined previous research in the literature on electronic identity (eID) credentials technologies and the projects carried out in Europe. We focused, especially on server-based e-signing methods. In the light of these reviews, we examined the applicability of a server-based mobile electronic signature model without disrupting local initiatives as a case study on the example of Turkey. Our analysis found that although Turkish citizens' identity cards have an e-signature infrastructure, this feature is not yet widely used. In Turkey's current eID structure, it is seen that different types of electronic signature solutions are tried to be implemented in various sectors and applications. However, none of them seem to have spread as planned. To address the adoption (Marsalek et al., 2017) problem in Turkey, we made a detailed analysis of the Austrian server-based eID approach, a combination of national identity cards and mobile signatures. As eIDAS allows the use of remote signing services that manage keys on behalf of service users, we have identified the primary requirements to evolve the eID infrastructure of the current Turkish eID plan towards a server-based approach. It has been observed that a server-based eID scheme can be achieved by making some changes in the existing Turkish eID structure, taking into account the existing structure and needs. It was concluded that the proposed eID structure is applicable to Turkey's legal and technical frameworks. The proposed centralized eID architecture does not provide a more secure environment than existing QES solutions (Theuermann, Tauber & Lenz, 2019), but all industries/applications (private or public) can benefit from a higher user experience. In addition, server-based solutions are based on a centrally implemented SSCD that is shared among all users. Storing and processing security-critical data in a secure central environment will also facilitate the management of the system. In conclusion, the proposed e-signature approach offers practical solutions to problems in usability and cross-border interoperability. Mobile devices, which are the most critical components of the server-based e-signature system, are widely used in societies today. With this high prevalence, using a server-based electronic signature with a mobile/electronic card may be the e-signature technology of the future. Government and private sector actors must work together to achieve a server-based e-signature system. Integration should be established between the country's central registration authority and certificate authorities, and legal regulations should be brought in line with international standards. During the study, the Austrian system and its applicability to Turkey were investigated. A significant difference between population sizes in this process (approximately nine times the population of Austria) revealed a possible technical performance limitation problem. It was concluded that more advanced and additional distributed systems could be considered to offer a solution to this problem (the distributed HSM design could be adapted to overcome the performance bottleneck). In summary, this study revealed that a server-based eID approach would contribute to developing a more user-friendly and flexible solution, but significant efforts still must be made to drive broad adoption.

ADDITIONAL INFORMATION AND DECLARATIONS

Funding

The authors received no funding for this work.

Competing Interests

Ozgun Erdogan is an employee of Innova Information Technology Solutions.

Author Contributions

- Ozgun Erdogan conceived and designed the experiments, performed the experiments, analyzed the data, performed the computation work, prepared figures and/or tables, authored or reviewed drafts of the paper, and approved the final draft.
- Nurdan Ayse Saran conceived and designed the experiments, analyzed the data, performed the computation work, authored or reviewed drafts of the paper, and approved the final draft.

Data Availability

The following information was supplied regarding data availability:

This is a literature review.

REFERENCES

Aciobanitei I, Dedita V, Pura M-L, Patriciu V-V. 2020. Sabres-a proof of concept for enhanced cloud qualified electronic signatures. In: *2020 13th International Conference on Communications (COMM)*. 103–108.

Aciobanitei I, Luculescu I, Pura M-L. 2020. Qualified electronic signature SAAS solution for Google Docs Google Sheets documents. In: *2020 13th International Conference on Communications (COMM)*. 109–112.

Activity Report 2018. 2018. Btk 2018 faaliyet raporu. *Available at https://www.btk.gov.tr/uploads/announcements/bilgi-teknolojileri-ve-iletisim-kurumu-2018-faaliyet-raporu-yayimladi/faaliyet-raporu-2018.pdf*.

Aichholzer G, Strauß S. 2010. The Austrian case: multi-card concept and the relationship between citizen id and social security cards. *Identity in the Information Society* **3(1)**:65–85 DOI 10.1007/s12394-010-0048-9.

Behrens C. 2012. Success factors for an e-government strategy: Austrian experiences, indonesian challenges. *Jurnal Studi Pemerintahan* **3(1)**:29–44.

Blind K, Gauch S. 2009. The demand for e-government standards. In: *Information Communication Technology Standardization for E-Business Sectors: Integrating Supply and Demand Factors*. Pennsylvania: IGI Global, 9–23.

Dumortier J, Vandezande N. 2012. Trust in the proposed EU regulation on trust services? *Computer Law & Security Review* **28(5)**:568–576 DOI 10.1016/j.clsr.2012.07.010.

Dzikrullah F, Rinjani MA. 2017. A framework design to develop integrated data system for smart e-government based on big data technology. *Bulletin of Social Informatics Theory and Application* **1(2)**:41–51 DOI 10.31763/businta.v1i2.26.

EGIZ. 2009. E-Government innovation center. *Available at https://joinup.ec.europa.eu/collection/e-government-innovation-center-egiz*.

Eichholtzer M. 2009. Large scale pilots. *Available at https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Large+Scale+Pilots* (accessed 3 February 2020).

eIDAS. 2009. EIDAS. *Available at https://www.eid.as/*.

FORMIT. 2013. Esignature study on the supply side of EU e-signature market-final study report. *Available at https://www.researchgate.net/publication/263304956_eSignature_-_Study_on_the_supply_side_of_EU_e-signature_market_-_Final_Study_Report_by_Formit*.

General Directorate of Population and Citizenship Affairs of Turkey. 2019. Tc Içişleri bakanlıgı-nüfus ve vatandaslik Işleri genel müdürlügü-tc kimlik kartı. *Available at https://www.nvi.gov.tr/*.

Gómez de la Cruz E. 2005. The electronic signature in Spain. *Digital Evidence and Electronic Signature Law Review* **2**:77.

Göransson A. 2018. *Electronic identification as an enabling or obstructive force: the general public's use and reflections on the Swedish e-ID*. Digitala Vetenskapliga Arkivet. *Available at http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1236665&dswid=-4097*.

GSMA. 2018. The mobile economy Europe. 2018. *Available at https://www.gsma.com/r/mobileeconomy/europe/*.

Han B, Chai Y, Liu Y. 2012. A study on trusted internet identity management and its application. In: *Advances in Electronic Engineering, Communication and Management.* Vol. 1. Berlin: Springer, 471–476.

Hühnlein D. 2014. Towards eIDAS as a service. In: Reimer H, Pohlmann N, Schneider W, eds. *ISSE, 2014 Securing Electronic Business Processes*. Wiesbaden: Springer Fachmedien Wiesbaden, 241–248.

Huhnlein D, Frosch T, Schwenk J, Piswanger C-M, Sel M, Hühnlein T, Wich T, Nemmert D, Lottes R, Baszanowski S, Zeuner V, Rauh M, Somorovsky J, Mladenov V, Condovici C. 2016. FutureTrust services for trustworthy global transactions. In: *Open Identity Summit 2016*.

Hühnlein D, Wich T, Hühnlein T, Schuberth S, Lottes R, Crossley N, Otto F. 2019. How to harmonise local and remote signing. In: *Open Identity Summit 2019*.

Information Society Statistics. 2011. 2011 bilgi toplumu istatistikleri. *Available at http://www.bilgitoplumu.gov.tr/wp-content/uploads/2014/04/Bilgi_Toplumu_Istatistikleri_2011.pdf*.

ITU. 2016. Expert group meeting on mobile id. *Available at https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2016/mID/Expert-Group-Meeting-on-Mobile-ID.aspx*.

Kabasakal D. 2007. *Elektronik Imzadan mobil elektronik imzaya geçiş Sürecindeki Yansumalar, Uygulamalar ve Öneriler*. Ankara: Bilgi Teknolojileri ve Iletişim Kurumu.

Kubach M, Leitold H, Roßnagel H, Schunck CH, Talamo M. 2015. Ssedic. 2020 on mobile eID. In: *Open Identity Summit 2015*.

Leenes R, Priem B, van de Wiel C, Owczynik K. 2009. Towards Pan-European recognition of electronic IDs-deliverable 2.2-report on legal interoperability. *Available at https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj–KrH0bDzAhUSnBQKHVXeDQgQFnoECAcQAQ&url=https%3A%2F%2Fec.europa.eu%2Fcefdigital%2Fwiki%2Fdownload%2Fattachments%2F78558114%2FD2.2_final..pdf%3Fversion%3D1%26modificationDate%3D1552336498893%26api%3Dv2&usg=AOvVaw0jwNWTd4CV0paL0LzjoP1i*.

Leitold H. 2011. Challenges of eID interoperability: the Stork Project. *Available at https://link.springer.com/chapter/10.1007/978-3-642-20769-3_12*.

Leitold H, Konrad D. 2019. Qualified remote signatures-solutions, its certification, and use. In: *Proceedings of 29th SmartCard Workshop*. 219–231.

Leitold H, Posch R. 2012. Stork-technical approach and privacy. In: *Digital Enlightenment Yearbook 2012*. Amsterdam: IOS Press, 289–306.

Lenz T, Stranacher K, Zefferer T. 2013. Enhancing the modularity and applicability of web-based signature-verification tools. In: *International Conference on Web Information Systems and Technologies*. Cham: Springer, 173–188.

Lenz T, Zwattendorfer B. 2016. Towards cross-border authorization in European eID federations. In: *2016 IEEE Trustcom/BigDataSE/ISPA*. Piscataway: IEEE, 426–434.

Liu-Jimenez J, Sanchez-Reillo R, Blanco-Gonzalo R, Fernandez-Saavedra B. 2015. Making stronger identity for EU citizens. In: *2015 International Carnahan Conference on Security Technology (ICCST)*. Piscataway: IEEE, 333–339.

Mariën I, Van Audenhove L. 2010. The belgian e-id and its complex path to implementation and innovational change. *Identity in the Information Society* **3(1)**:27–41.

Marsalek A, Zefferer T, Reimair F, Karabat Ç, Soykan EU. 2017. Leveraging the adoption of electronic identities and electronic-signature solutions in Europe. In: *Proceedings of the Symposium on Applied Computing*. 69–71.

Melin U, Axelsson K, Söderström F. 2016. Managing the development of e-id in a public e-service context: Challenges and path dependencies from a life-cycle perspective. In: *Transforming Government: People, Process and Policy*. Bingley: Emerald Publishing.

Mocanu S, Chiriac AM, Popa C, Dobrescu R, Saru D. 2019. Identification and trust techniques compatible with eIDAS regulation. In: Li J, Liu Z, Peng H, eds. *Security and Privacy in New Computing Environments. SPNCE 2019. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*. Vol. 284. Cham: Springer.

Mutlugün M, Adalier O. 2009. Turkish national electronic identity card. In: *Proceedings of the 2nd International Conference on Security of Information and Networks*. 14–18.

Myhr T. 2008. Legal and organizational challenges and solutions for achieving a pan-european electronic id solution: or i am 621216–1318, but i am also 161262–43774. do you know who i am? *Information Security Technical Report* **13(2)**:76–82.

Nikolouzou ESKIASG. 2020. eIDAS compliant eID solutions. *Available at https://www.enisa.europa.eu/publications/eidas-compliant-eid-solutions*.

Nyman T, Ekberg J-E, Asokan N. 2014. Citizen electronic identities using TPM 2.0. In: *Proceedings of the 4th International Workshop on Trustworthy Embedded Devices*. 37–48.

Orthacker C, Centner M, Kittl C. 2010. Qualified mobile server signature. In: *IFIP International Information Security Conference*. Springer, 103–111.

Patel C, Joshi D, Doshi N, Veeramuthu A, Jhaveri R. 2020. An enhanced approach for three factor remote user authentication in multi-server environment. *Journal of Intelligent & Fuzzy Systems* **39(Preprint)**:1–12.

Paulin A. 2012. Status and outlook on electronic idenitity in europe: the case of austria. In: *IFIP e-Government Conference 2012*. 71–80.

Polanski P. 2015. Towards the single digital market for e-identification and trust services. *Computer Law & Security Review* **31(6)**:773–781 DOI 10.1016/j.clsr.2015.09.001.

Protopappas L, Sideridis AB, Yialouris CP. 2020. Implementation issues of cross border e-government systems and services. In: *HAICTA*. 155–166.

Quarterly Market Data Report. 2019. Türkiye elektronik haberleşme sektörü-Üç aylık pazar verileri raporu. *Available at https://www.btk.gov.tr/duyurular/turkiye-elektronik-haberlesme-sektoru-3-aylik-pazar-verileri-raporu-yayimlandi*.

Rath C, Roth S, Bratko H, Zefferer T. 2015. Encryption-based second authentication factor solutions for qualified server-side signature creation. In: *International Conference on Electronic Government and the Information Systems Perspective*. Springer, 71–85.

Rath C, Roth S, Schallar M, Zefferer T. 2014. Design and application of a secure and flexible server-based mobile eID and e-signature solution. *International Journal on Advances in Security* **7**:50–61.

Rissanen T. 2010. Electronic identity in Finland: ID cards vs. bank IDs. *Identity in the Information Society* **3(1)**:175–194 DOI 10.1007/s12394-010-0049-8.

Rivera A, Milena A, Kristjan V. 2015. Estonia-A successfully integrated population-registration and identity management system: delivering public services effectively. *Available at https://documents.worldbank.org/en/publication/documents-reports/documentdetail/873061495178335850/estonia-a-successfully-integrated-population-registration-and-identity-management-system-delivering-public-services-effectively*.

Rosca V. 2017. Exploring barriers to mobile e-id adoption: a government perspective on republic of moldova mobile e-ID. *Available at https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1115928&dswid=-1552.*

Roßnagel H, Camenisch J, Fritsch L, Gross T, Houdeau D, Hühnlein D, Lehmann A, Shamah J. 2012. Shaping the future of electronic identity. *Datenschutz und Datensicherheit* **36(3)**:189–194.

Ruica E-C, Pura M-L, Aciobanitei I. 2020. Implementing cloud qualified electronic signatures for documents using available cryptographic libraries: a survey. In: *2020 13th International Conference on Communications (COMM)*. 113–118.

Ruiz-Martínez A, Sánchez-Martínez D, Martínez-Montesinos Mia F, F. Gómez-Skarmeta A. 2007. A survey of electronic signature solutions in mobile devices. *Journal of Theoretical and Applied Electronic Commerce Research* **2(3)**:94–109 DOI 10.3390/jtaer2030024.

Sagıroglu S, Kabasal D, Alkan M. 2008. Mobil elektronik Imza,altyapss ve tükiye. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi* **1**:49–56.

Sealed D, Piper A. 2007. Study on the standardisation aspects of esignature. IDABC Report.

SecSign. 2019. Two-factor-authentication. *Available at https://www.secsign.com/business/two-factor-authentication*.

Sedek KA, Sulaiman S, Omar MA. 2011. A systematic literature review of interoperable architecture for e-government portals. In: *2011 Malaysian Conference in Software Engineering*. Piscataway: IEEE, 82–87.

Sideridis AB, Costopoulou CI, Yialouris CP, Savvas I, Maliappis MT, Ntaliani M, Karetsos S, Tsiafoulis SG, Protopappas L, Chatziandreou A. 2017. Cross-border e-government authentication services. In: *HAICTA*. 850–864.

Soyez S. 2019. Metadata and the digital transition: the case of the belgian "digital act". *Archives et Bibliothèques de Belgique-Archief-en Bibliotheekwezen in België* **106**:75–82.

Stipsits T, Kammerstetter M. 2015. Security analysis of the Austrian citizen card environment mocca and e-card. *Available at https://www.auto.tuwien.ac.at/bib/pdf_TR/TR0174.pdf*.

Stranacher K, Zefferer T, Tauber A, Zwattendorfer B. 2013. The Austrian identity ecosystem: an e-government experience. In: *Architectures and Protocols for Secure Information Technology Infrastructures*. Pennsylvania: IGI Global, 289–309.

Strauß S, Aichholzer G. 2010. National electronic identity management: the challenge of a citizen-centric approach beyond technical design. *International Journal on Ad-vances in Intelligent Systems* **3(1)**:12–23.

Sullivan C. 2018. Digital identity-from emergent legal concept to new reality. *Computer Law & Security Review* **34**:723–731.

Szadeczky T. 2018. Enhanced functionality brings new privacy and security issues-an analysis of eID. *Masaryk University Journal of Law and Technology* **12(1)**:3–27.

Tang M, Alazab M, Luo Y. 2017. Big data for cybersecurity: vulnerability disclosure trends and dependencies. *IEEE Transactions on Big Data* **5(3)**:317–329.

Theuermann K, Tauber A, Lenz T. 2019. Mobile-only solution for server-based qualified electronic signatures. In: *ICC, 2019 IEEE International Conference on Communications (ICC)*. Piscataway: IEEE, 1–7.

Wang X, Jiang J, Zhao S, Bai L. 2019. A fair blind signature scheme to revoke malicious vehicles in vanets. *Computers, Materials & Continua* **58(1)**:249–262 DOI 10.32604/cmc.2019.04088.

Werle R, Iversen EJ. 2006. Promoting legitimacy in technical standardization. *Science, Technology & Innovation Studies* **2(1)**:19–39.

Yin RK. 2009. *Case study research: design and methods*. Thousand Oaks: Sage Publications.

Zefferer T. 2014. A server-based signature solution for mobile devices. In: *Proceedings of the 12th International Conference on Advances in Mobile Computing and Multimedia*. 175–184.

Zefferer T, Krnjic V, Stranacher K, Zwattendorfer B. 2014. Measuring usability to improve the efficiency of electronic signature-based e-government solutions. In: *Measuring E-government Efficiency*. Berlin: Springer, 45–74.

Zhang J, Xiao H. 2020. An efficient and practical quantum blind signature protocol with relaxed security model. *Computers, Materials & Continua* **63(1)**:301–313 DOI 10.32604/cmc.2020.07681.