



A SERVER BASED ELECTRONIC SIGNATURE APPROACH TO IMPROVE
E-SIGNATURE PRACTICES IN TURKEY

ÖZGÜN ERDOĞAN

JANUARY, 2020

A SERVER BASED ELECTRONIC SIGNATURE APPROACH TO IMPROVE
E-SIGNATURE PRACTICES IN TURKEY

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED
SCIENCES OF
ÇANKAYA UNIVERSITY

BY

ÖZGÜN ERDOĞAN

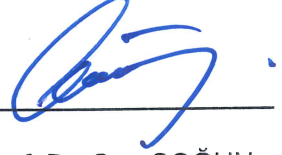
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE
DEGREE OF
MASTER OF SCIENCE
AT INFORMATION TECHNOLOGIES
DEPARTMENT

JANUARY 2020

Title of the Thesis: **A Server Based Electronic Signature Approach to Improve E-Signature Practices in Turkey**

Submitted by **Özgün ERDOĞAN**

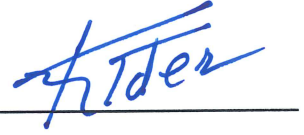
Approval of the Graduate School of Natural and Applied Sciences, Çankaya University.



Prof. Dr. Can ÇOĞUN

Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.



Prof. Dr. Sıtkı Kemal İDER

Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.



Assist. Prof. Ayşe Nurdan SARAN

Supervisor

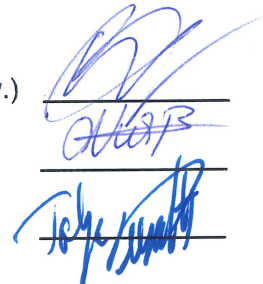
Examination Date: 03.01.2020

Examining Committee Members

Assoc. Prof. İhsan Tolga MEDENİ (Ankara Yıldırım Beyazıt Univ.)

Assist. Prof. Ayşe Nurdan SARAN (Çankaya Univ.)

Assoc. Prof. Özgür Tolga PUSATLI (Çankaya Univ.)



STATEMENT OF NON-PLAGIARISM

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name : Özgün ERDOĞAN

Signature :



Date

: 07.02.2020

ABSTRACT

A SERVER BASED ELECTRONIC SIGNATURE APPROACH TO IMPROVE E-SIGNATURE PRACTICES IN TURKEY

ERDOĞAN, Özgün

M.Sc., Department of Information Technologies

Supervisor: Assit. Prof. Ayşe Nurdan SARAN

January 2020, 95 pages

In this study, a server-based electronic signature structure has been investigated as a valid and centralized e-signature method in terms of its applicability to Turkey's current eID structure. Current widespread e-signature methods' and their applications that are in use in Turkey are examined further, so that possible advantages and disadvantages of a new server-based solution can be determined clearly. Research specifically contains the Austria's server-based eID approach that is in use and continues with the compatibility assessment of the requirements of this solution with Turkish eID usecases. Hence, a possible server-based eID structure for Turkish eID environment is proposed and the applicability of this server-based e-signature method is evaluated in the context of whether it can ease Turkish practices of e-signing. Necessary steps to achieve a successful integration of the presented solution to the current infrastructure are determined. It is concluded that, server-based signature approach would contribute to the development of a more usable and cross-border way of online identification as well as it would help to reach the international standards of e-signatures in Turkey.

Keywords: Austrian Server-Based eID, eID, Mobile Signature, Server-Based E-Signatures, Turkish eID

ÖZ

TÜRKİYE'DE E-İMZA UYGULAMALARININ GELİŞTİRİLMESİ İÇİN SUNUCU TABANLI ELEKTRONİK BİR E-İMZA YAKLAŞIMI

ERDOĞAN, Özgün

Yüksek Lisans, Bilgi Teknolojileri Anabilim Dalı

Tez Danışmanı: Dr. Ayşe Nurdan SARAN

Ocak 2020, 95 sayfa

Bu çalışmada geçerli ve merkezi bir imzalama yöntemi olarak sunucu tabanlı elektronik imzalama yöntemi ve bu yöntemin Türkiye'nin mevcut elektronik kimlik yapısına uygulanabilirliği araştırılmıştır. Bu methodun avantaj ve dezavantajlarını açık bir biçimde belirleyebilmek için, günümüzde Türkiye'de yaygın kullanımda olan e-imza metodları ve uygulamaları detaylı bir şekilde incelenmiştir. Araştırma özellikle Avusturya'da kullanımda olan sunucu tabanlı çözümü kapsamakta ve bu çözümün gereksinimlerinin Türkiye'deki e-imza senaryolarına uygunluk değerlendirmesi ile devam etmektedir. Çalışmaların sonucu olarak, Türkiye için sunucu bazlı bir elektronik kimlik altyapısı önerilmiş ve bu merkezi e-imza altyapısının uygulanabilirliği Türkiye'deki e-imza uygulamalarını kolaylaştırma bağlamında değerlendirilmiştir. Sunulan yöntemin mevcut altyapıya başarılı entegrasyonu için gerekli adımlar belirlenmiştir. Sunucu bazlı elektronik imza yaklaşımının, Türkiye'de daha kullanışlı ve uluslararası bir kimlik doğrulama yönteminin geliştirilmesine ve bunun yanı sıra Türkiye'deki e-imzaların uluslararası standartlara ulaşmasına yardımcı olacağı sonucuna varılmıştır.

Anahtar Kelimeler: Avusturya Sunucu Tabanlı Elektronik Kimlik, Elektronik Kimlik, Mobil İmza, Sunucu Tabanlı Elektronik İmza, Türkiye Elektronik Kimlik

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to Dr. Ayşe Nurdan SARAN for his supervision, special guidance, suggestions, and encouragement through the development of this thesis.

It is a pleasure to express my special thanks to my family for their valuable support.

TABLE OF CONTENTS

STATEMENT OF NON-PLAGIARISM.....	iii
ABSTRACT.....	iv
ÖZ.....	v
ACKNOWLEDGEMENTS.....	vi
TABLE OF CONTENTS.....	vii
LIST OF FIGURES.....	ix
LIST OF TABLES.....	xi
LIST OF ABBREVIATIONS.....	xii
CHAPTERS:	
1. INTRODUCTION.....	1
1.1. Problem Statement.....	1
1.2. Background.....	2
1.3. Solution Statement and Contribution.....	4
1.4. Organizations of the Thesis.....	4
2. LITERATURE REVIEW.....	6
2.1. Two-Factor Authentication.....	7
2.2. Different Typologies and Usecases of E-Signatures in Countries.....	8
2.2.1. Two-Factor Authentication with Smart Cards.....	9
2.2.2. Mobile Two-Factor Authentication Methods.....	10
2.2.3. Server-Based Mobile Two-Factor Authentication Method.....	11
2.2.4. National ID Card Based Two-Factor Authentication Method (Citizens Cards)	12

2.3.	Cross-Border Identification of Users and Global Projects	14
3.	E-IDENTITY IN TURKEY	22
3.1.	Overview of the Current Available Methods of E-Signing In Turkey	30
3.1.1.	Secret Password Methods	31
3.1.2.	Smart Card Based Methods	35
3.1.3.	Mobile Methods.....	42
3.1.4.	National ID Cards.....	46
3.1.5.	oAuth	50
4.	A SERVER-BASED E-SIGNATURE METHODOLOGY THAT CAN IMPROVE THE E-SIGNING PROCESSES IN TURKEY	53
4.1.	Server-Based E-Signing Methodology	53
4.2.	Austrian eID Ecosystem	54
4.2.1.	Austrian Server-Based Signatures (Mobile Phone Signature)	56
4.2.2.	A Modular Approach to Austrian Server-Based Signatures	58
5.	PROPOSED eID STRUCTURE AND USECASES FOR TURKEY.....	63
5.1.	Requirements Analysis for Turkey's EID Structure	64
5.2.	Proposed eID Structure and Usecases for Turkey	69
5.3.	Applicability of the Proposed Method.....	79
5.3.1.	Legal Framework	79
5.3.2.	Technical Framework.....	81
5.3.3.	Security Framework	82
5.4.	Contribution to the Current EID Structure of Turkey.....	84
6.	CONCLUSION.....	90
	REFERENCES	92

LIST OF FIGURES

FIGURES

Figure 1 Two-Factor Authentication Scheme [4]	8
Figure 2 FUTUREID Infrastructure [20].....	18
Figure 3 FutureTrust System Architecture [7].....	20
Figure 4 Internet Access Rates of Enterprises After 2005 [31].....	23
Figure 5 Electronic Service Delivery Levels in EU-27 + Countries, 2010 [31].....	25
Figure 6 Public Information And Communication Technology Investment Allocation [31]	26
Figure 7 Electronic Signature Usage Rates in Enterprises in the year 2010 [31].....	28
Figure 8 Secret Password Login page of Turkish E-Government Application [38]...32	
Figure 9 Secret-Password Usecases in General.....	33
Figure 10 Total Electronic and Mobile Electronic Signature Certificate Numbers in Years [39]	34
Figure 11 Smart Card Based Login Page of Turkish E-Government Application [38]	35
Figure 12 Smart-Card Based E-Signature Usecase in Turkey	36
Figure 13 Interface of the Software of E-Tuğra Information Technologies and Services Inc. [40]	39
Figure 14 Interface of the Software of Scientific and Technological Research Council of Turkey [41].....	39
Figure 15 Interface of the Software of TURKTRUST Information Security Services Inc. [42].....	40
Figure 16 Dongles of Scientific and Technological Research Council of Turkey [41]	40
Figure 17 Dongles of TURKTRUST Information Security Services Inc. [42].....	41
Figure 18 SIM Card Based Mobile Signature Usecases in Turkey	44
Figure 19 Mobile Electronic Signature Login Page of Turkish E-Government Application [38].....	45
Figure 20 Mobile Application Login Page of Turkish E-Government [38].....	46
Figure 21 National ID Card Based e-Signature Usecase in Turkey	48
Figure 22 National ID Card Login Page of Turkish E-Government Application [38].49	
Figure 23 oAuth Login Page of Turkish E-Government Application [38].....	50
Figure 24 oAuth Mechanism via Banks in Turkey	51
Figure 25 eID Ecosystem in Austria [13]	54
Figure 26 MOA-ID Template [48].....	55
Figure 27 MOCCA Local Architecture [16]	56
Figure 28 MOCCA Online Architecture [16]	56
Figure 29 Austrian Mobile Phone Signature Architecture [16]	57
Figure 30 Mobile Phone Signature Interfaces provided by A-SIT [48]	57
Figure 31 Overview of Components of Rath et al.'s Method [15].....	58

Figure 32 Registration Process of Austrian Mobile Signature Proposed by Rath et al. [15]	60
Figure 33 Activation Process of Austrian Mobile Signature Proposed by Rath et al. [15]	61
Figure 34 Usage Process of Austrian Mobile Signature Proposed by Rath et al. [15]	62
Figure 35 Interface of the Usage Process of Rath et al. [15]	62
Figure 36 Proposed eID Infrastructure for Turkey	69
Figure 37 Proposed Registration and Usage Usecases for Citizen Card Signatures for Turkey	70
Figure 38 Proposed Registration and Usage Usecases for Server-Based Signatures for Turkey	71
Figure 39 Security Evaluation Results of MOCCA [16]	84
Figure 40 e-Government Benchmark Report 2018 Country Factsheet for Turkey [52]	85
Figure 41 e-Government Benchmark Report 2018 Country Factsheet for Austria [52]	86
Figure 42 Perceived Usability of Different Implementations of Austrian e-Government [16]	88

LIST OF TABLES

TABLES

Table 1 STORK Project Pilot Services [5]	16
Table 2 STORK 2.0 Project Pilot Services [5]	17
Table 3 Turkish eID Structure in 2019.....	29

LIST OF ABBREVIATIONS

Ades	Advanced Electronic Signatures
Certification Authority (CA)	Entity that issues digital certificates. In this model of trust relationships
Certification Service Provider (CSP)	Entity or legal or natural person who issues digital certificates or provides trust services related to electronic signatures
eID	Electronic Identity
eIDAS	Regulation “on electronic identification and trusted services for electronic transactions in the internal market”
e-SENS	Electronic Simple European Networked Services
EU	European Union
STORK	Secure Identity Across Borders Linked
Trust Service Provider (TSP)	Entity which provides one or more electronic Trust Services
Trusted List (TL)	List indicating the supervision/accreditation status of certification services of Certification Services Providers who are supervised/accredited by the reference Member State for compliance with the provisions laid down in Directive 1999/93/EC.
QES	Qualified Electronic Signatures

CHAPTER 1

1. INTRODUCTION

1.1. Problem Statement

In order to provide more alternatives of identity validation for the Turkish people; private sector and the Turkish government try to adapt with the new solutions of identity validation arising from different technological developments such as two-factor authentication, mobile technologies continuously. While these new technologies are implemented to 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 this heterogeneous implementation styles is considered as the lack of clarity in terms of implementation in Directive 1999/93/EC [1] [2], which is community framework for electronic signatures prepared by European Parliament. Different e-signature technologies arise from these heterogeneous implementations cause usability problems as much as they present an obstacle in front of Turkey's journey to establish an eID structure that supports cross-border identity validation.

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 different online services everyday. For example in Turkey, some of the governmental services require smartcard based e-signatures such as e-prescriptions services used by doctors in health sector. 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, they have different passwords for each legal bank accounts because their bank may not provide electronic signature login option. As a result, people are obliged to manage all these different passwords and identification documents in their daily lives. It is also mentioned in the paper named *“Estonia: A Successfully Integrated Population-*

Registration and Identity Management System” that; fragmentation is a common problem with the identification systems [3]. They mentioned how separating identification structures to satisfy sector-specific demands without establishing standards causes fragmentation [3].

Result is, same basic information are collected from the users repeatedly and used for authentication purposes in separate databases of institutions such as government institutions, hospitals, telecom companies and banks. Since there are no standards to integrate those adequately, users have to manage different password for each of them.

Besides usability problems Turkish users are facing, existence of different e-signature technologies results in different technical structures needed to be combined to establish a Turkish eID environment capable of cross-border validation. eSignature Final Study Report by FORMIT Foundation states the impacts of different e-signature implementations on eID as follows [1]. They explained the situation as “*Existence of different typologies of e-signature has allowed Member States to apply the Directive with certain degrees of freedom, generating more confusion than opportunities in cases that require interoperability across the national boundaries*” [1] and they concluded “*In the near future current national institutional frameworks will have to face challenging tasks such as cross-border interoperability of Related Trust Services*” in their concluding remarks [1].

In other words; in course of adding different implementations and sector-based solutions more and more to provide alternatives for identity validation; the usability of the general system is getting more complex for the end users and it is getting harder to reach an international and easy way of online identification in Turkey.

1.2. Background

Majority of online services has adopted single secret passwords as authentication method and it is still on use. Electronic identities (eID) and electronic signatures introduced to us as online identity management concepts providing a sufficient level of security and usability during the past years. However, the security factor has gained importance since electronic identities are used for handling governmental and administrative official procedures or services.

To meet the security requirements, two-factor authentication concept introduced to us allowing the users securely identify themselves by the help of factors possession and knowledge [4]. Along with the developments in two-factor authentication schemes, different e-signature technologies discovered such as identification via smart card methods, mobile methods, citizen card concept etc.. With the introduction of Directive 1999/93/EC that is Community Framework for Electronic Signatures prepared by European Parliament [2], e-signatures that meet certain conditions became legally equivalent to the wet signatures [2]. In order to get the most benefit from electronic signatures, countries formed their own country-based usecases immediately. After 2007, sphere of influence is extended and pilot projects like STORK, STORK 2.0 and e-SENS are given start by EU organizations to support the cross-border identity validation [5]. With the help of these successful projects, a basis for eIDAS regulation towards cross-border electronic identification is tried to be constituted. As electronic identification and trust services for international electronic transactions schemes have been introduced with the eIDAS regulation in 2014 [6], researchers once again give some thought to an international concept of eID and face with the problem of different implementations in different countries. A global project named FUTURETRUST continues aiming a simpler and international way of online identification scheme [7].

In the meantime in Turkey, Electronic Signature Law No. 5070 imposed in 2004 [8] and as a beginning four certification authorities are authorized for handling the electronic signature operations [9]. After 2007, mobile electronic signatures and different solutions started to be implemented all over the country. [9] Turkey recently have put into use the national citizen card system and the countrywide transformation continues [10]. Besides national ID card system; dongle based methods, SIM cards based methods and recently oAuth methods are still in use to authenticate users in Turkey. Currently six electronic signature certification authority and three telecom company continues to serve Turkish citizens with various e-signature solutions [11]. On the other hand, despite the eIDAS regulation effective from 2016, there have been no change made in Turkey's e-signature law yet to comply with the eIDAS regulation. During the ongoing process of national citizen cards and studies towards new e-signature law in 2019, necessary steps to achieve more usable and international way of online identification is investigated in this thesis.

1.3. Solution Statement and Contribution

To achieve an international and more usable way of online identification for Turkey, server-based eID solutions are examined in this study. An alternative server-based eID structure is presented and measures needed to be taken to establish this structure in Turkey are identified. The presented server-based method and usecase developed for Turkey's eID structure provides a solution for enabling the infrastructure of Turkey to be international and more advanced in terms of usability.

1.4. Organizations of the Thesis

This thesis contains six chapters. Necessary information about the server-based e-signature solution is presented; advantages and disadvantages of the centralized design of this method are explained. The applicability of this centralized method of e-signing is evaluated in the context of whether it can ease Turkish practices of e-signing.

Chapter 1 is an introduction to the history of e-signature processes and objectives of this thesis.

Chapter 2 is the literature review section and it includes information about the different techniques of e-signature used by different countries, which embraced different usecases. Server-based eID structures and international projects aiming cross-border interoperability of eID are further investigated.

In Chapter 3, currently used Turkish identity validation methods and their usecases are investigated. The components of these techniques are examined and difficulties with the usability of these methods are presented.

In Chapter 4, a server-based e-signature solution based on Austria's eID scheme that can ease the e-signing processes is discussed in today's context of Turkish practices. Key components of the Austrian eID ecosystem are identified.

Chapter 5 includes a requirements analysis for Turkey's eID scheme. An eID structure and usecases that enables the server-based e-signatures in Turkey is presented. Steps to integrate a server-based e-signature method in the existing structure of Turkey's are discussed, the parts that need to be improved are identified.

Applicability and security of the method is discussed. Contributions to the current identity validation scheme are explained.

Chapter 6 summarizes the outputs and deductions of the study.

XCPS
GCPS

CHAPTER 2

2. LITERATURE REVIEW

Nowadays, the use of electronic identities is an obligation as much as it is a necessity especially in domains like e-government, e-business and e-health. As 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 more secure and usable work environment. According to FORMIT Foundation's report, e-government concept is one of the primary focus on the European agenda [1]. Report mentions that the member states have announced plans for a more open, accessible and transparent administration, using the latest technologies for electronic signature [1]. Throughout the implementations of latest technologies in the countries, different typologies of e-signatures are formed in each country. Moreover, with the different e-signature solutions used in different sectors, sector-based solutions and usecase are formed. In Turkey's case, course of events were similar. Alternative and sector-specific identity validation methods based on electronic signatures were implemented without establishing any common standards with other countries. These sector and country based implementations in Turkey causes problems in terms of usability and cross-border operability. In order to provide a solution for these problems; this research draws upon findings from prior research on widespread eID systems in countries, in particular on server-based e-signing methods, and international eID projects conducted within Europe.

Although the usability factor and cross-border electronic identification are more concentrated on in this study; the security factor is an inseparable and constant part of the e-signing concept, as electronic signatures are legally equivalent to handwritten signatures according to the Directive 1999/93/EC of the European Union [2]. One of the biggest breakthrough of identity validation schemes in terms of security is probably achieved by two-factor authentication concept. All valid e-signature technologies

adopted by countries are based on this concept because the infrastructure of all subsequent solutions is based on two-factor authentication.

2.1. Two-Factor Authentication

To mention first, authentication is a commonly used term in eID related concepts. However, identification is also used in this domain. The difference in their definitions between these terms explained as follows.

Identification - is explained as the provision and transfer of all characteristics of an entity, here natural person (e.g. name, address, e-mail address) to the Relying Party [12].

Authentication - is the recognition of a natural person – usually it is the login at a legal authority [12]. An authenticated user simply means that the user is legitimized by the Relying Party for a particular service [12]. For this reason, in eID schemes, use cases includes verification steps in which the Relying Party transmits data to the e-identity providers for verification.

Two-factor authentication concept is an important concept as it is introduced to the literature in order to increase the security level on systems and inholds several implementation styles to improve compatibility. Simply, it is a method that a combination of two different factors, possession and knowledge, is used to confirm users' claimed identities [4]. Possession term explains the ownership of the private key [4]. It says basically that every person have to possess their own key [4]. Knowledge is explained as the person should have a secret PIN/Password to use his /her private key [4]. It can't be processed without his/her knowledge since PIN/Password only known by him/her [4]. In some cases, knowledge factor can be obtained by biometric data of the users too. [4] Figure 1 shows the Two-Factor Authentication components.

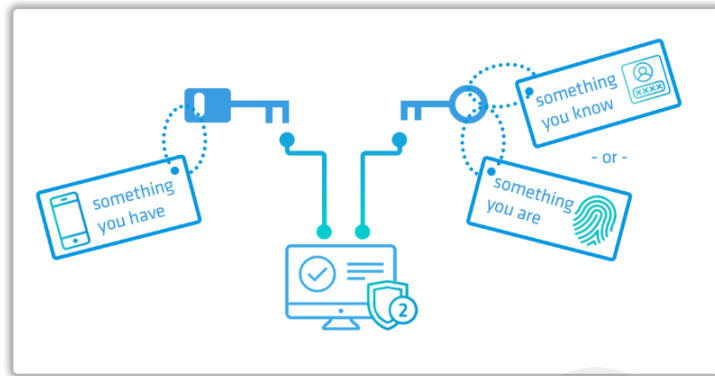


Figure 1 Two-Factor Authentication Scheme [4]

On the grounds of this concept, different typologies of two-factor authentication are presented over the years with respect to the developments and trends in the e-signature concepts such as mobilization, cross-border identification etc.. In order to provide a secure environment for e-signature processes, solutions combined with two factor authentication such as e-signatures via smart cards, mobile two factor authentication with SIM cards and server-based mobile two factor authentication methods are implemented earlier and they are still in use in different countries.

2.2. Different Typologies and Usecases of E-Signatures in Countries

During past years, different concepts of electronic signing are introduced such as Two-Factor Authentication with Dongle Method (smart card contains the private key/ID), Mobile Two-Factor Authentication Method (SIM card contains the private key/ID) or ID Card Based Two-Factor Authentication Method (Citizens cards with e-signature capability). The concepts are chosen by countries in terms of their applicability to the countries' unique eID structures. Nevertheless, countries are in tendency to create their unique usecases when it comes to the application of these methods. One of the main reason of this heterogeneity between countries' usecases is considered as the lack of clarity in terms of implementation in the Directive 1999/93/EC of the European Union according to the FORMIT Foundation's report [1]. Besides that, this directive has been inadequate to provide a clear legal landscape for national eIDs too, since it covers electronic signatures only [2]. Recently, eIDAS regulation has been put in use in 2016 [6]. eIDAS replaced the old regulation with the provision of qualified trust services for the validation and preservation of electronic

signatures as well as the cross-border recognition of electronic identification schemes [6]. While some countries have legally completed their studies to comply with the new directive, some countries are still working. However, current eID solutions are not yet available in a standardized and interoperable manner within Europe.

As a result; different national eID schemes exist across the Union, from smart card based architectures where government issues different national smart cards for each citizen [3] [13], to SIM based or server-based mobile architectures where mobile phones are an integral part of the solutions in some way [14]. For this reason, examining each application scenario of e-signing in these countries in detail gives perspective and provides understanding to problems of usability and cross-border operability. In the next part, these e-signing methods are explained. Classification of the electronic signature solutions is made according to their implementation styles.

2.2.1. Two-Factor Authentication with Smart Cards

Smart card based authentication schemes have been a very popular way of Two-Factor Authentication implementation around Europe [15]. The authentication process is based on possession and knowledge factors while possession means actual ownership of eID token via smart cards and knowledge is reached by having the specific secret PIN/Password that protects access to the token inside the card [13].

Alongside of the adequate level of security of smart card based authentication, they are found to lack an appropriate level of usability because of some of the disadvantages of it [16] [15]. The necessity for card-reading devices in combination with the associated software were some of these disadvantages discussed by Zefferer in 2012 [16] [15]. However, according to the research conducted, Two-Factor Authentication with Dongle Method seems to be very stable and still preferred method among countries despite its low level of usability [1]. Some time ago, the only solution presented to people was dongle solution and it was the first viable solution for electronic signing. Because of being the first, it seems that it became the regular practice in time. In time as other solutions are presented, people could not abandon their habit easily because it is not easy to accept new usecases. As “e-Signature Final Study Report” by FORMIT Foundation informs, the use of new solutions are started to increase in various countries but it can't be said that it is sufficiently widespread [1].

2.2.2. Mobile Two-Factor Authentication Methods

Recent developments in mobile communication technologies form a basis for mobile two-factor authentication method that enables authentication through mobile phones. Method is based on the grounds of mobile phones providing the possession of eID token via SIM Cards [15]. SIM-based mobile solutions usually require a special SIM card, as off-the shelf SIMs do not support necessary cryptographic operations [15]. A secret PIN protects the eID data stored on the SIM while SIM is under the possession of the user himself/herself [15]. This way, SIM-based solutions rely on two different authentication factors. With the realization of two-factor authentication concept via mobile phones, usability factor is highly improved with a sufficient level of security.

There are also major drawbacks of the mobile electronic signature solutions mentioned in several studies. One limitation of the existing mobile eID and e-signature solutions discussed is that their dependence to specific use cases [15]. According to Rath et al. most mobile eID and e-signature solutions do not have a specific use case and because of that, the use of these solutions is very difficult in different fields of application [15].

Another disadvantage concerns the SIM cards in the sense of security. According to Ruiz-Martínez et al., *“mobile handsets have reached a significant penetration rate in many countries such as Luxemburg (164%), Italy (128%), Hong Kong (117%), Spain (109%), Chile (74%), Argentina (64%), and so on.”* [17]. That is why security measures are very important in mobile e-signature solutions today. It is discussed that; since cryptographic operations (creation of electronic signatures) are carried out on the user’s mobile device, these cryptographic operations and private data that is processed in that device, have a risk of malware exposure [15] [18]. This issue was considered important especially, popular smartphone platforms such as Android found to be vulnerable against malware [15] [18].

Another important problem with the mobile phones’ SIM cards is the dependence of the card manufacturer on the creation and stamp of the symmetric keys [17]. Since manufacturers are different, usecases and security measures of these companies are also different. For example in Turkey; three main telecom company provides SIM cards that is able to perform electronic signatures so there is no common standard on production of SIM cards. Additionally, some government applications need specific e-signatures provided by specific certification authority in Turkey.

Because of that, people may not be able to use these applications with their personal mobile signatures if their telecom company uses a different certification authority's e-signatures.

2.2.3. Server-Based Mobile Two-Factor Authentication Method

Server-based authentication methods promise less complex structure to its users due to its usability and security features [19] [15]. Due to these advantages, the concentration was on server-based methods and their applications during this research. In the review of different architectural models for eIDs, countries where server-based identification methods are in use were focused.

By taking into consideration the problems with current applicable methods in Turkey, the usability factor and the cross-border electronic identification, Orthacker et al.'s Mobile Server Signature concept is reviewed in detail [19]. Orthacker et al.'s method simply depends on a concept that cryptographic operations are handled in hardware security modules (HSMs) instead of users' local environment like SIM cards or smart cards [19]. Because of Orthacker et al.'s solution is already have implemented in Austrian e-Government applications since November 2009 [15], method also seems very strong in terms of applicability. Orthacker et al.'s solution is also very important due to its compliance with the EU Directive 1999/93/EC [2] and it is already proven since the method has been in productive operation in Austria for several years [15] [19]

Orthacker et al. identifies *"lack of applications for electronic signatures"* as one of the factors for the low market penetration of qualified signatures in their research [19]. In order to provide a solution to this problem, Rath et al. proposed a modular and flexible server-based e-signature method that can ease the method's integration to applications in 2014 [15]. According to Rath et al., *"existing mobile solutions are usually tailored to the requirements of specific use cases and fields of application"* [15]. This leads to situations, in which most applications cannot benefit from these mobile solutions [15]. To overcome the problem, Rath et al. presented a flexible server-based solution that is based on Orthacker et al.'s grounds of implementing a secure hardware element [19]. In this solution, cryptographic operations all carried out in a Hardware Security Module as well [19] [15]. However, the infrastructure introduced by the study provides more flexible authentication environment regarding

external components to users [15]. This flexibility is fulfilled on architectural level which is consist of two parts (inner part and outer part) [15].

The implementation of Austrian eID scheme (national smart cards & server-based combination) [13] and its usability evaluation conducted by Zefferer are investigated [16]. In the Zefferer et al.'s study, the security and trustworthiness of the eID system named MOCCA and its' usecases are also evaluated [16]. MOCCA system includes three sub solutions which are a local solution, an online solution and a server-based solution [16]. They concluded in their study that, the server-based sub solution of the Austrian case appears to be the most secure and trustworthy solution, followed by Local and Online sub solutions [16].

2.2.4. National ID Card Based Two-Factor Authentication Method (Citizens Cards)

Citizen card concept is actually a smart card based solution that adopts Two-Factor Authentication concept and includes an ID Card Chip, SMS, Card-reading machine, PIN/Password in its e-signature process. Since most of the countries used ID Cards with no digital information and no chips before the online worlds existed, people have formed a habit of having an actual physical item under their hands. The practicality and advantage of the ID cards is also mentioned in the work "*Estonia: A Successfully Integrated Population-Registration and Identity Management System*" as its convenient size allows it fit better than a passport into a regular wallet and they are valid for identification in most of the European Union countries [3]. The practicality of it made ID Cards convenient to integrate with new solutions. Therefore, countries prosecute the ID Cards solutions by adding more features such as containing data of fingerprint and biometric information of one. In most cases, ID cards of the users do not only provide identification but also authentication by enabling users to create electronic signatures [20].

A lot of countries have adopted national ID Card based identification and authentication method over the past decades including EU member states Finland, Belgium, Estonia, Austria, Sweden, Italy, Spain, Portugal and Germany etc. [20]. In Estonia, the first national ID card with digital signatures were used in October 2002 [3]. Estonia also constitutes a good example with its successful integration system that connects the population register records with eID systems [3]. Project named X-Road completed with the collaboration of private companies, IT firms, and commercial

Banks in Estonia so that interconnection between the Population Register (PR) and identification management systems (IDMS) is established [3]. The X-Road platform is a good example of Public-Private Partnership as well as central and standardized data exchange platform [3].

Another country where national ID cards with e-signatures are issued to allow citizens to securely identify and authenticate at online procedures, is Austria [13]. National cards have been in use since 2002 and they have been designed to be applicable in both the public and the private sector [13]. According to the research, Austrian identity ecosystem is also designed with a central component called MOA-ID that provides secure identification and authentication of citizens [13]. With the help of MOA-ID and several components together, population register authority of Austria and different types of eID services are connected [13].

Latest developments in Turkey includes national identity card system too. Since 2017, citizen cards have been distributed to citizens also in Turkey through general directorate of population and citizenship affairs [10].

Although ID Card Based Method is the direction most countries seems 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 [7]. However, Estonia's and Austrian e-identity schemes can be a good example handling this problem [3] [13]. In Estonia, with the e-residency program supported by the X-Road platform, identification and authentication of the foreigners is made possible [3]. The Austrian government also introduced national card concept to its citizens but then they improve their system towards server-based mobile eID strategies over the years supporting cross-border identification of users [13]. The key point is here is that, Estonia and Austria developed an integration model ensuring development of a unified system [3] [13]. With a unified and centralized system, Austrian and Estonian e-government systems also constitute a base for cross-border identification of citizens. Because of that, their usacases and experiences are very significant for other countries.

Another resource, which is relevant to the Austrian's e-Government solution, is the bachelor's thesis named "*Security Analysis of the Austrian Citizen Card Environment MOCCA and E-Card*" belonging to Thomas Johannes Stipsits from the Faculty of Informatics at the Vienna University of Technology [21]. Thomas introduced the MOCCA and examined the procedure of a signature creation of it [21]. As a result,

the study showed that the only significant weakness of the system is that it is vulnerable to the fake applet attacks which is hard to perform [21].

2.3. Cross-Border Identification of Users and Global Projects

Cross-border identification is one of the popular subjects discussed in EU organizations lately. The integration of countries' systems with each other and the sharing of information between systems gained importance once the countries settled on the concept of eID within their own structures. However, as different technologies introduced to literature such as two-factor, multi-factor, server-based signing or biometric identity validation concepts; number of different usecases and variation between countries schemes are increased. Consequently, cross-border operability of the countries' eID schemes tried to be achieved especially in Europe.

Studies to establish a legal framework at European level produced results and Directive 1999/93/EC, which enables electronic signatures to become legally recognized within the Member States, is established [2]. Turkey's e-signature regulation named Electronic Signature Law No. 5070 is established at 23 January 2004 complying with this regulation [8]. Recently, 2014/910/EU eIDAS regulation is put into force since 1st July 2016 in Europe [6]. eIDAS regulation replaces the old eSignature Directive (1999/93/EC) and any inconsistencies in Digital Signature law across Europe [6] [22]. eIDAS regulation is introduced aiming to ensure that countries' national electronic identification schemes are also valid in other EU countries where qualified e-signatures are available. After eIDAS come into force, Turkey gave a start to the transition process of Turkish e-signature law like other countries. Although Turkey is not a European Union country, studies continue in order to achieve a compatible eID environment with Europe as it mentioned in the information and communication technologies authority's activity report [23]. Turkey also involved in most of the international projects concerning cross-border identification [5].

The difference between the Directive 1999/93/EC and 2014/910/EU eIDAS regulation is very important in terms of changes in fundamentals of eID concepts. The eSignature Directive (Directive 1999/93/EC) has been around for fifteen years and lacks many definitions and procedures [2]. However, eIDAS regulation comes with three definitions of Electronic Signatures [6].

General Electronic Signatures

eIDAS provides the basis for all electronic signatures, arguing that electronic signatures cannot be denied legally just because of their electronic form [6].

Advanced Electronic Signatures (AdES)

AdES must be uniquely linked to the signer and authorities should be able to identify the signer [6]. Signers create their signatures using only the data under their control and the final output is strictly protected against interference [6].

Qualified Electronic Signatures (QES)

QES is a more strict type of AdES. For electronic signatures to pass the QES qualifications, they must be created using a Digital Certificate purchased from a “*trust services provider*”, such as a Certificate Authority (CA) [6]. It is the only type of signature that has the same legal value as wet signatures across Europe according to eIDAS [6]. Both AdES and QES prove identity of the signer and are the equivalent of wet ink signatures [6]. The main difference between them is that AdES can be accepted by other EU member states, but QES must be accepted [6].

An important outcome is that; while the old directive also does not take into account new technologies that have developed since its implementation [22], eIDAS allows the use of different technologies such as server-based e-signing services in order to manage private keys on behalf of the users [6] [22]. With server-based signing, signing keys are held on a service provider’s HSM. With this approach, the need for users to handle their own private keys is eliminated [6]. In short, eIDAS reduces bureaucracy, makes processes less costly, and makes the lives of individuals and companies easier.

Along with these developments in legal frameworks, international projects were initiated among European countries. Some of the important project that are successfully completed so far are STORK [24], STORK 2.0 [5], FUTUREID [20], e-SENS [5] and FUTURETRUST [7]. Although these projects are carried out by different organizations from EU, their common mission were developing common specifications for secure and mutual recognition of national electronic identities (eID) between countries. These projects chosen to be investigated because they are large-scale projects involving many countries and pilot projects between these countries [5].

STORK

STORK (Secure Identity across Borders Linked) project was one of the first project that aims providing secure access to public services across EU borders. STORK is an EU co-funded project executed between June, 2008 to December, 2011 [25] [26]. The main issue the STORK project wanted to address was the heterogeneous nature of eID in Europe [24]. Main achievements of the STORK project can be summarized in four subjects; common specifications, quality authentication assurance (QAA) levels, a common code and pilot cross-border e-Services [26]. As for common specifications, minimum requirements to put in practice an eID infrastructure and to establish the cross-border authentication platform have been defined on legal, organizational and some technical areas [26]. Besides these requirements, while acknowledging the different existing policies and procedures of countries, STORK QAA levels were defined to create a mapping to a common model [26]. Also, a common code were created by STORK project aiming an integration between connected parties [26].

In the field of interoperability, STORK project provided six pilots running since summer 2010 [5]. Pilot projects and their specific domains can be seen in table 1.

Table 1 STORK Project Pilot Services [5]

Project	Domain
Cross-border Authentication for Electronic Services	For electronic services
Safer Chat	To promote safe use of the Internet by children and young people
Student Mobility	To help people who want to study in different Member States
Electronic Delivery	To develop cross-border mechanisms for secure online delivery of documents
Change of Address https://www.eid-stork.eu/pilots/pilot5.htm	To assist people moving across EU borders
ECAS (European Commission Authentication Service) Integration	ECAS Integration

18 Member States and Associated Countries of the European Union with over 25 cross-border e-Government identity services piloted these solutions [26]. The STORK project includes 35 consortium partners however; Turkey has not been involved in this project.

STORK 2.0

Following the success of the STORK project, these studies are transferred to the STORK 2.0 project [5]. STORK 2.0 project started in 2012 and 57 partner institution, both public and private, across 19 European countries are involved [26]. STORK 2.0 is introduced as a pan-European project that allows citizens to identify themselves across borders by using their eID data from authentic and reliable sources in the context of different business domains [5]. This project conducted in collaboration with ISA, CEF and the eIDAS to define the standards and building blocks for cross-border eID interoperability complying with the eIDAS Regulation so that more sustainable solution is can be provided [26]. STORK 2.0 was completed in the year 2015 [24].

Major achievements have been accomplished with STORK 2.0 such as; common specifications are studied by the member states, an open source infrastructure based on the common specifications was made available for EU Member States and four pilot applications have been demonstrated to validate projects' common specifications, standards and building blocks [5]. These pilot projects shown in table 2, were important because they address the challenges in governance issues (across borders, different application domains and sectors) in practice. STORK 2.0 Pilots, focused on domains like eLearning and Academic Qualifications, e-Banking, and e-Health areas [5].

Table 2 STORK 2.0 Project Pilot Services [5]

Project	Domain
e-Academia	Cross-border academic services
e-Banking	Pan-European online banking services supporting national eIDs
e-Gov4Business	Access to foreign public e-Services (PSC) on behalf of a legal entity
e-Health	Cross-border exchange of European citizens' health data

On the contrary of the STORK project, Turkey participated in the two of the pilot projects within the STORK 2.0. Turkey has been one of the countries contributing the e-Academia and e-Health projects [5].

FUTUREID

FUTUREID project started with the idea that; federated identity management approach to national electronic identity card schemes already existing in countries may help to achieve stronger authentication [20]. The challenges addressed in the FUTUREID project were; *“No standardized, trustworthy and ubiquitously usable eID client”, “Complex and costly integration of authentication and identity services”, “No coherent European trust infrastructure for authentication”, “Privacy threats of real world authentication solutions”, “Non-technical problems”* [20].

FUTUREID project aimed to provide an integrating framework across Europe and beyond and two pilot applications were developed during the project to demonstrate the applicability of the developed technologies [20].

As a result of the FUTUREID project, interoperability of eID systems are improved. The project contributed to overcome the fragmentation and complexity of the eID landscape [20]. A simple infrastructure aimed in the FUTUREID project is shown in the figure 2.

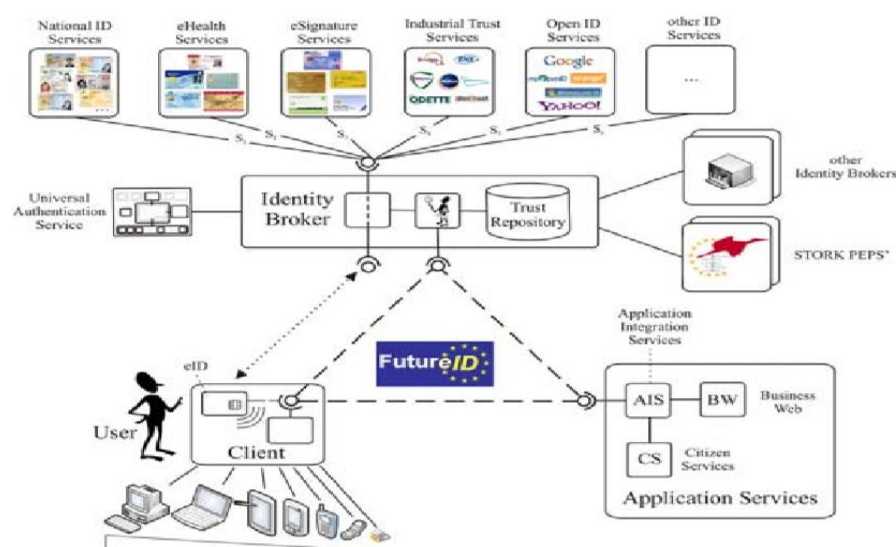


Figure 2 FUTUREID Infrastructure [20]

eSENS

eSENS (Electronic Simple European Networked Services) project was launched in 2013 by the European Commission to provide a technical base for cross-border identification issues manifested in the previous projects like STORK [5]. Previous projects have tended to address existing eID issues by focusing on a single domain such as delivering e-health, e-education or judicial services. However, with the eSENS project, it is aimed that bringing together the results of these individual projects and delivering building blocks that can be used to develop solutions across a range of sectors. [5] Project continued between the years 2013 and 2017 and 65 pilot project across over 18 countries were implemented [5] .

Another key advantage that eSENS provides to public administrations and service providers was building blocks for developing e-delivery solutions fulfill the technical requirements of the EU electronic identification and trust services (eIDAS) regulation [5].

eSENS project is completed on 31 March 2017 [5]. Among many successful activities eSENS has; a cross-border digital identity (eID) framework, an eIDAS/STORK plugin, evaluations of different trust establishment models and an open source environment for implementations of eSENS were the eSENS's main technical developments have been validated in a variety of domains [5]. Also, the first cross-border and eIDAS compliant connection is achieved through eSENS project connecting the electronic identification and authentication infrastructures of Germany, Netherlands and Austria in 2017 [27]. For example; farmers can authenticate themselves using their own eID and log in to the countries' portals cross-border with the structure provided by eSENS project [28].

FutureTrust

A project named FutureTrust funded by EEMA (The European Association for e-Identity & Security) within the EU Framework Program for Research and Innovation (Horizon 2020) is an ongoing project since its' start June 1st 2016, in collaboration with European countries [7]. The project's core objective is to support the practical implementation of the eIDAS regulation (2014/910/EU) on electronic identification (eID). FutureTrust aims to provide a solution for cross-border recognition of electronic identification benefiting from the developments in remote and mobile signing services,

in which no local secure signature creation device is needed and cryptographic operations are handled by central Hardware Security Modules (HSMs) hosted by a trusted service [7]. FutureTrust project is the most recent international project that deals with the cross-border authentication issue, which Turkey participated. As one of the players in Turkish e-signature market, Scientific and Technological Research Council of Turkey (TUBİTAK-UEKAE) is one of the partners supporting the FutureTrust project [7]. FutureTrust project's system architecture is given in the figure 3 below.

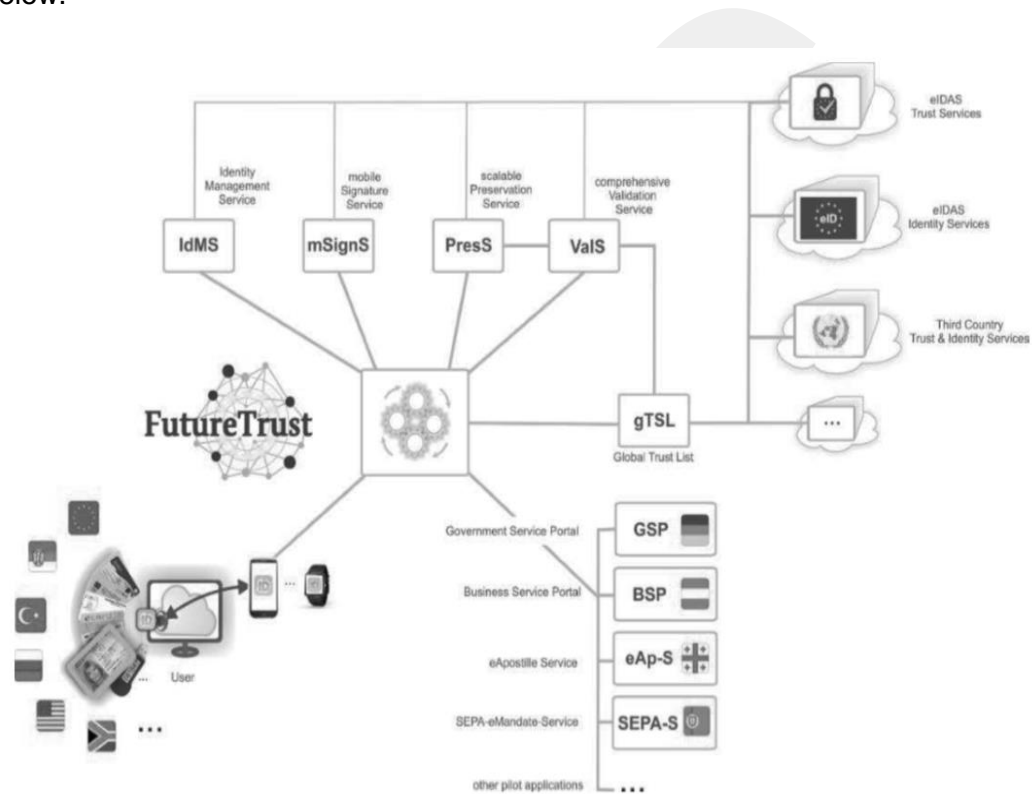


Figure 3 FutureTrust System Architecture [7]

One of the problems that FutureTrust project deals is explained as, “the first part of the eIDAS regulation that deals with eID management systems aims to create a standardized interoperability framework but does not intend to harmonize the respective national eIDM systems of countries.” [1]. It is also a motivation for this study since no country will take on responsibility to create a comprehensive solution for everyone. Each country needs to take concrete steps and prepare their own infrastructures to reach an integrable solution at the end.

Recently in 2019, FutureTrust project reached the point of demonstrating their pilot applications to the world [29]. These pilot projects are Portuguese service for

electronic SEPA e-Mandates (e-Mandates), Austrian service for electronic invoices (e-Invoice), Georgian service for electronic apostilles (e-Apostille) and German eIDAS-Portal that allows users to enroll after an eID-based authentication [29].

With all the projects carried out, Turkey has endeavored to create and develop its eID system according to the latest developments by acting together with other European countries. Turkey participated in STORK 2.0, eSENS, and FutureTrust projects. In addition to that, Turkey's and other countries' e-government progression is also monitored by the latest progression reports of the EU [30].

On the other hand, these international projects aims interoperability between countries systems and establish common standards. They do not provide any solution to improve countries' specific systems for them. Each country has its own tasks to be completed on that account. In order to create a cross-border authentication environment for Turkey, first step would be clarifying the authentication scheme of Turkey.

CHAPTER 3

3. E-IDENTITY IN TURKEY

As the importance of online security increased in the presence of illegal transactions and fraud over the years, providing more secure solutions to customers became a responsibility of everyone including citizens, governments and private sector. Major steps were taken by governments to maintain the security of online services against drawbacks of single password-based solutions and authentication schemes in the last 20 years. Despite the e-identity issue is more adopted by European countries, Turkey also has started to participate to the studies about online identification since 2002. After the preparations of an electronic signature law and the introduction of the Electronic Signature Law No. 5070 in Turkey [8]; electronic signatures, which ensures the validity, integrity, accessibility and undeniability of the transactions carried out in electronic environment, has started to be used since 2004 [8].

In 2004, four companies were endowed with the authority to serve as a certification authority in Turkey [8] [11], these companies were;

- TURKTRUST Information Security Services Inc. (TürkTrust Bilgi, İletişim ve Bilişim Güvenliği Hizmetleri)
- E-Güven Information Security Inc. (Elektronik Bilgi Güvenliği A.Ş.)
- Scientific And Technological Research Council Of Turkey (TUBİTAK-UEKAE)
- E-Tuğra Information Technologies and Services Inc. (EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.)

With the initiatives of these four companies and the support of the government, the smartcard based electronic signature (dongles contain smartcards) solution was made ready for Turkish citizens in 2004. Since then, Turkish citizens have been using these smartcards in their online activities. Today, the number of certification authority raised to six with Security General Directorate Certification Center (EGMSM) and E-Signature Information Security Services Inc. (e-İmzaTR) entering the picture in 2012 and 2013 [11]. These six companies continue to provide smartcard based electronic

signatures, which is a qualified electronic signature (QES), to users and public employees.

When we look at the internet availability conditions in Turkey, compared with the EU enterprises, it is observed from the Turkish Statistical Institute's studies shown in the figure 4 that internet access rate in Turkey has increased and come close to the average internet access levels of EU countries (AB-27, AB-25 and AB-15 representing subgroups of EU countries) after 2005 [31].



Figure 4 Internet Access Rates of Enterprises After 2005 [31]

In addition to the increase in internet access of enterprises in Turkey after 2005, with the availability of secure e-signature solutions, public institutions and organizations have started to develop projects in order to provide public services to citizens with maximum quality and minimum cost and to reduce bureaucratic transactions by carrying out transactions with related parties in e-signed form. According to the research conducted in 2007 by Kabasakal [9], 19 government institutions were applied to Scientific and Technological Research Council of Turkey (TUBİTAK-UEKAE) to obtain qualified signature certificates in 2007 [9]. We can draw a conclusion that internet availability increase over the years was one of the factors, which enhanced the demand for electronic signatures in Turkey.

As internet usage increased over the years, Turkish government enhanced its support on online and secure electronic activities. Government institutions have started to use the electronic signatures both in their correspondence and in the services they provide to citizens and businesses. As of 13 May 2011, Scientific and Technological Research

Council of Turkey (TUBİTAK-UEKAE) issued 144,707 qualified electronic certificates for the usage of government personnel [31].

Besides these studies, developments on e-government applications have accelerated since 2005 in Turkey. Electronic government (e-government) provides a participatory, transparent and accountable government structure fulfils the needs of citizens and provides integrated services whereby users can access public services from a single point. With its characteristics, e-government is one of the most important tools for effectively managing electronic transactions countrywide.

The e-government project of Turkey, which aims to provide joint public services from a single point, became operational on 18 December 2008 with 22 services [31]. At the end of 2010, the number of services provided through the e-Government Gateway reached 246 [31]. On the other hand, the number of users in the system increased significantly; the number of registered users reached 1.95 million at the end of 2010 and 7.14 million at the beginning of May 2011 according to the Turkish Statistical Institute's reports [31].

Along with the efforts made at the country level, comparisons also were made at the international level. According to Turkish Statistical Institute's report, 9th e-Government Measurement and Benchmarking Study, which the EU has carried out regularly since 2001, was held in 2010 [31]. The study covers 32 countries in total, 27 EU member countries together with Turkey, Croatia, Iceland, Norway and Switzerland (EU-27 +) [31]. According to the results of this study, Turkey's Electronic Service Delivery Level was above the average of the countries' levels in the year 2010 [31]. Service delivery levels of countries in the year 2010 can be seen in figure 5 [31].

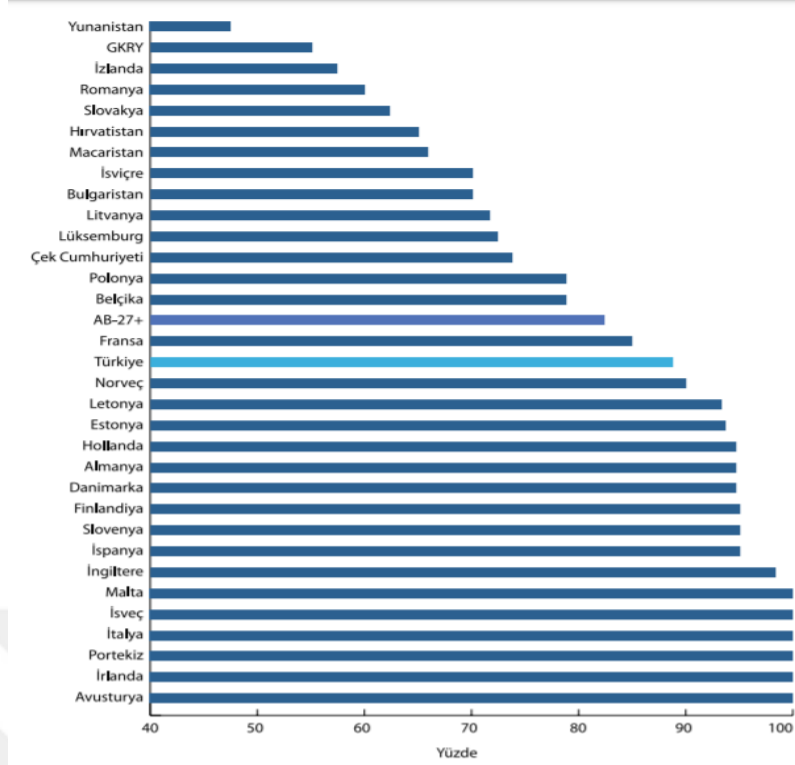


Figure 5 Electronic Service Delivery Levels in EU-27 + Countries, 2010 [31]

According to the 2018 Digital Government Factsheets report prepared by European commission; the number of services provided through the e-Government portal increased significantly since January 2017 and reached to 3,027 services [32]. Although there are many reasons and increasing factors, this increase is mostly a result of 2016 - 2019 National e-Government Strategy and Action Plan [32]. For the provision of the Strategy and Action Plan, a procurement contract is signed with Scientific and Technological Research Council of Turkey (TUBİTAK-UEKAE) [32].

The 2016-2019 National e-Government Strategy and Action Plan is an important step in Turkey's e-identity studies because it is the first comprehensive national e-government study that coordinates and benefits from different other studies new technological developments and global trends [32]. This program included the studies covering status analysis, review of national strategies, review of relevant legislation and international best practices, as well [32]. 4 strategic aims, 13 objectives and 43 actions have been determined to achieve the vision of an e-Government ecosystem, the aims are being; "Ensuring Efficiency and Sustainability of the e-Government Ecosystem", "Implementing Common Systems for Infrastructure and Administrative Services", "Realizing e-Transformation in Public Services", "Enhancing Usage, Participation and Transparency" [32].

On the other hand, the Information Society Strategy and Action Plan for years 2015 – 2018 was approved and published by the High Planning Council on 6 March 2015 [32]. This program mainly focused on achieving the aim of providing efficiency and adopting the principle of user centrality when delivering e-Services [32]. While 2016-2019 National e-Government Strategy and Action Plan mostly focused on the public sector, Information Society Strategy and Action Plan focused on the society and private sectors.

Besides these national programs of e-government in Turkey, the aim of establishing an e-government structure that is in accordance with user needs, user oriented, collaborative, integrated and reliable, is also covered in the Turkey's Tenth Development Plan for the years 2014 to 2018 [32]. An important approach of the plan was obtain an integration between e-government and public sector information systems such as central registration system(CRS) ,electronic public procurement platform (EPPP) etc. [32]. This way establishing a shared infrastructure and setting common standards in terms of e-signing are aimed [32].

Digital transformation is never easy without a help from government. Turkish government, besides its e-government actions, manage and monitor the public institutions' electronic signature transition. With the help of government and major investments made in last fifteen years, the internet and the electronic signature usage have been increased [31]. We can see investments in information technologies made by public institutions between the years 2002 and 2011 below in figure 6 [31].

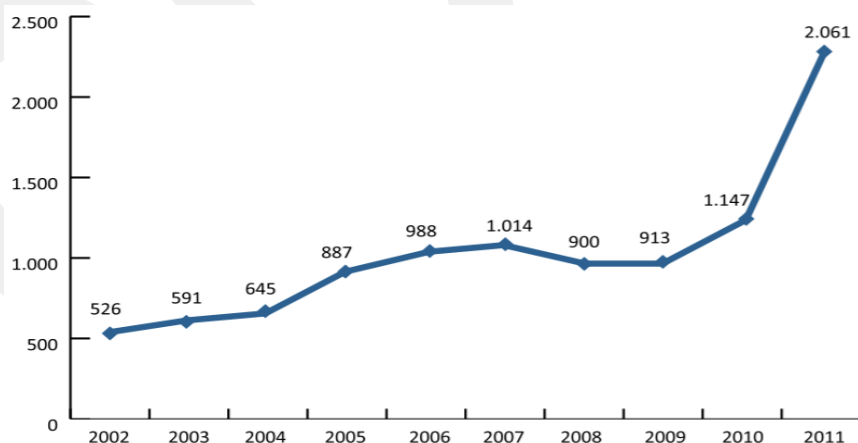


Figure 6 Public Information And Communication Technology Investment Allocation [31]

Over the years, smart card based electronic signatures could not become as widespread as desired all over world and also Turkey. Some of the reasons for that

explained as; lack of common e-signature software, location dependency due to card reader, smart card and related software in a fixed location, lack of necessary infrastructure and applications, high cost of transition and integration to electronic environments, low awareness/lack of awareness, the distrust of new technology etc. [9]. In addition to these factors, affecting the proliferation of smart card based electronic signatures negatively, increased mobile device penetration also triggered the mobile electronic signature studies all over the world. As a result of these studies, mobile e-signing technologies are introduced to the literature in 2007 [9]. In the proposed solution, cryptographic operations performed on the SIM cards located in the users' mobile devices. Integrating the smartcard functionality to the SIM cards and using mobile phones to store eID data securely was an innovative idea. Due to its advantages such as easy use of mobile e-signatures, low cost to the user and the possibility of signing independent of time and space, countries such as Norway, Finland, England, Poland, Sweden, Estonia, Lithuania and Germany have completed their studies and launched their mobile electronic signature work by 2008 [14]. Mobile electronic signature infrastructure was implemented with the help of telecommunication companies between the years 2007 and 2008 in Turkey. Turkcell was the first company that put into practice the mobile e-signature solution in 2007 after the introduction of Communiqué Amending the Communiqué on the Processes and Technical Criteria Regarding Electronic Signature [8], which is published in the official gazette, dated 26/06/2008 and numbered 26918.

Meanwhile, with the developments in mobile communication technologies, mobile phone subscriber density in Turkey reached 92.1% at the end of year 2008 with a rapid development; it stabilized at 83.9% by the end of 2010 [31]. All of these studies including e-government, e-signature dissemination in public institutions and mobile e-signature studies with telecom companies have contributed to the Turkey's electronic signing progress in those years.

According to the information society report released in 2011 by Turkish Statistical Institute, the rate of using electronic signature in enterprises was 26 percent for enterprises with 250+ employees in year 2010 as it seen in the figure 7.

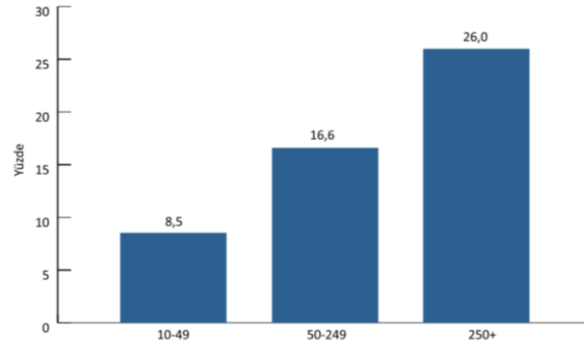


Figure 7 Electronic Signature Usage Rates in Enterprises in the year 2010 [31]

Today, three main telecom company continues to serve as a mobile e-signature supported SIM card provider in Turkey. These companies, Turkcell, Türk Telekom and Vodafone, provide mobile e-signature solutions and their services to Turkish citizens in collaboration with six electronic signature certification authorities.

Besides trending mobile solutions in last decade, various countries adopted national ID card based identification and authentication method. Especially in Europe, countries like Austria [33], Estonia [34], Belgium [35] or Spain [36] are some of countries that have issued personalized smart cards for their citizens allowing identify and authenticate themselves securely under the eyes of the government and law [15].

Turkey's citizen card studies started in 2008 with the project of Scientific and Technological Research Council of Turkey (TUBİTAK-UEKAE) [37]. Within the scope of this project, other countries' national identity card applications were examined, comparisons are made and pilot applications in some cities of Turkey were started to be carried out in 2009 [37]. Citizen cards officially started to be distributed to citizens all over the country through general directorate of population and citizenship affairs at the beginning of 2017 [10]. Citizen cards continue to be distributed in 2019 and the information of number reaching 37 Million (nearly half of the 82 million population in Turkey) was shared by the e-population union of public employees in 2019 [10].

For the year 2019, current Turkish eID structure can be summarized as below table 3;

Table 3 Turkish eID Structure in 2019

E-Signature Certification Authority	Signature Creation Device	Mobile E-Signature Partner	Target Customer Type
TURKTRUST Information Security Services Inc. (TürkTrust Bilgi, İletişim ve Bilişim Güvenliği Hizmetleri)	Smart Cards	-	Personal E-Signature
	SIM Cards	Vodafone	
Scientific And Technological Research Council Of Turkey (TUBİTAK-UEKAE)	Smart Cards	-	Personal E-Signature + Government Employees
	SIM Cards	Turkcell	Government Employees
	National ID Cards	-	Personal E-Signature + Government Employees
E-Güven Information Security Inc. (Elektronik Bilgi Güvenliği A.Ş.)	Smart Cards	-	Personal E-Signature
	SIM Cards	Turkcell Türk Telekom	
E-Tuğra Information Technologies and Services Inc. (EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.)	Smart Cards	-	Personal E-Signature
Security General Directorate Certification Center (EGMSM)	Smart Cards	-	Personal E-Signature
e-İmzaTR Information Security Services Inc. (e-İmzaTR Bilgi Güvenliği Hizmetleri A.Ş.)	Smart Cards	-	Personal E-Signature

Over the years, all of the above-mentioned solutions brought into use in Turkey due to their advantages. In addition to above-listed ways of identity validation, Turkish citizens can login their e-government accounts with two other methods as well. One of them is the oldest way, login with a single secret passwords. Turkish citizens who acquire their e-government password, can login their online e-government account with a single secret password without a second control mechanism. Another way to identify a user in Turkish e-government site is oAuth mechanism supported by the banks. E-government site has integrated their system with about 30 banks to provide an oAuth mechanism to the Turkish citizens. Since banks are official institutions from the eyes of government, e-identities that exist in banks' system can be counted as a valid online identity of the person.

To provide an eID environment that is simple and usable for the citizens, the government and private sector services have to change and adapt their e-signing substructure with all of the new solutions individually. However, different organizations adopting different e-signature solutions increases general system's complexity. Besides that, the requirements of these new technologies can ensue as software or hardware requirements, which hardens eID providers' and individual's adaption processes. Having too many passwords to remember for one person for different services makes the process unusable. The need of a simple and inclusive method of identity authentication arise day by day under these circumstances in Turkey. Therefore, providing an architecture with higher usability and possibly an international solution for identity authentication is aimed in this thesis.

To identify the strong and week points of Turkish eID structure, current Turkish usecases further examined against best practices applied by other countries in this section. The aim of this approach is finding the most applicable and suitable improvement strategy to achieve more usable and cross-border form of e-signing in Turkey.

3.1. Overview of the Current Available Methods of E-Signing In Turkey

In this part of the study, available secure e-signing methods for a Turkish citizen to login the Turkish e-government application are investigated. Examining the usecases and profiles provides an understanding of the current Turkish eID infrastructure and users' habits. According to the 2018 Digital Government Factsheets report prepared

by European commission, the total number of registered users on the Turkey's e-government platform was 36,688,014 in 2018 [32]. Because of its countrywide comprehensiveness and its structure supporting all of the e-signature methods used in the recent period, Turkish e-government site and the use case scenarios of it were examined.

In e-government service, secure transactions are currently provided through five methods; secret passwords given to users upon request, smart card based electronic signatures, mobile electronic signatures, OAuth via internet banking and national ID cards [32].

3.1.1. Secret Password Methods

Identification via single secret passwords is still an identity validation mechanism available all over the internet. Method itself based on a usecase which individuals having a secret password for each system used and they are approved without a second confirmation mechanism. In spite of the developments in two-factor authentication methods, secret passwords are still a common choice of people and companies due to its usability and easy implementation.

If we look at the situation in Turkey closely, we see that there are many e-identification solutions implemented so far especially by the government institutions. Identification via smartcards, mobile phones, national eID cards are some of the methods that have been in use for years. After the year 2004, which is the year of Electronic Signature Law No. 5070 entered into force [8], many government institutions started to adopt this new technologies to improve their systems in terms of security [9].

However, secret password solution is never abandoned under the effects of these new authentication methods. It remained as a backup policy and continue to exist next to the other new solutions. This is because institutions, public or private, had their own databases to handle their operations and services at the beginning. There was no central authority to connect these institutions together and organize their operations to optimize the customers' processes so each institutions handled its operations on its own. After the introduction of the new customer based e-signature methods, institutions continued to keep their own databases even if they comply with the new technologies government proposed. There were simply two perspectives on

that issue. From the eyes of the customer; signing in via secret password is easy and fast and people continued the use their unique passwords within the institution no matter how secure is the other option. Moreover, usability, security, complexity and economical disadvantages of the newly introduced solutions, affect negatively their enlargement process. On the other hand, from the eyes of the institutions; the maintenance of a single database is easier, more economical and more manageable and comparing to modifying their system allowing other methods of e-signing and also they want to ease the signing process for the customer in order to preserve customer satisfaction level. The secret password signing method and its usecases for the Turkish e-government application is given below in figure 8 and 9 [38].

The screenshot shows the login interface for the Turkish E-Government Application. At the top, there is a header with the logo and text "e-Devlet Kapısı Kimlik Doğrulama Sistemi". Below this, there are two links: "Giriş Yapılacak Adres" pointing to "www.turkiye.gov.tr" and "Giriş Yapılacak Uygulama" pointing to "e-Devlet Kapısı". The "turkiye.gov.tr" logo is also present on the right. The main content area features a navigation bar with five options: "e-Devlet Şifresi", "Mobil İmza", "e-İmza", "T.C. Kimlik Kartı", and "İnternet Bankacılığı". Below the navigation bar, there is a text block: "T.C. Kimlik Numaranızı ve e-Devlet Şifrenizi kullanarak kimliğiniz doğrulandıktan sonra işleminize kaldığınız yerden devam edebilirsiniz." followed by a link "e-Devlet Şifresi Nedir, Nasıl Alınır?". The login form consists of two input fields: "* T.C. Kimlik No" and "* e-Devlet Şifresi". Each field has a "Sanal Klavye" (Virtual Keyboard) icon and a "Yazarken Gizle" (Hide while typing) icon. At the bottom of the form, there are two buttons: "İptal Et" (Cancel) and "Sisteme Giriş Yap" (Login to System).

Figure 8 Secret Password Login page of Turkish E-Government Application [38]

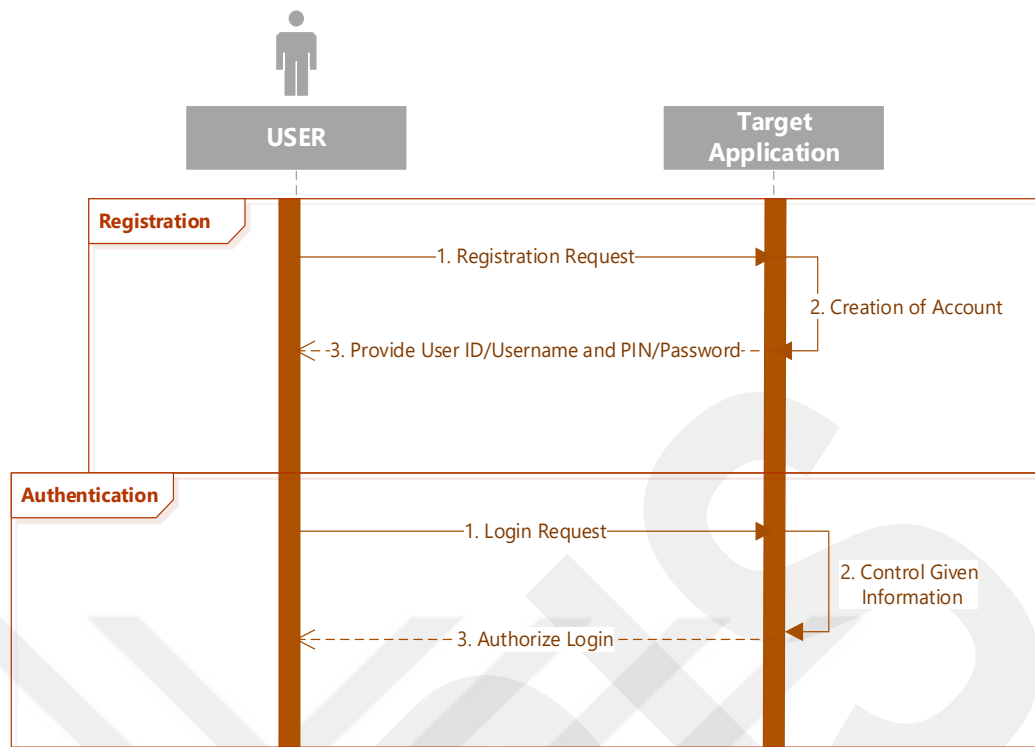


Figure 9 Secret-Password Usecases in General

Secret password structure is based on the grounds of separate databases. In this kind of structures, every individual can sign into the institutions' web sites and create an identity for himself. After the users provided the necessary information to create an identity, the institution provide a user ID or username and a PIN/password to the users and keep this information safe under its database which the security of it provided by institution itself. After registration face, users can login to the application using their user ID/username and secret password. All they need to do is send a login request online to the target application with the correct user ID/username and secret password information. There is no second control defined in the process. Unless there is a technical problem in the connection, login request of the users are authorized by the system. This type of identification of users corresponds to the general electronic signatures described in the eIDAS regulation [6].

As a result, separate databases of the institutions remain their existence. Although people understand the importance of the security factor, sometimes by experiencing security threats and finding themselves in difficult positions such as fraud, the usability factor never let the simple password solution disappear. Today, there are public institutions' services which qualified electronic signature usage is mandatory such as

national judiciary informatics system applications, creation of electronic prescriptions in medical systems, ministry of labor and social security application work permit application of foreigners etc. to ensure a certain security level in their services. Other than that, in important services such as bank sites, e-government site etc. signing in via secret passwords method still in use in Turkey. They continue to identify individuals by their online identities, which are specific to these online services.

Accordingly, the usage of two factor authentication methods such as authentication through dongles, mobile phones or national ID cards is still insufficient. According to the information and communication technologies authority's 2019 report data given in the figure 10; in the second quarter of 2019, the current total number of electronic signatures and mobile signatures are 3.59 million and 581 thousand respectively [39]. The number of electronic signatures increased by 4.1% and the number of mobile signatures increased by 2% compared to the previous period [8]. The Turkish population is 79.81 million (2016 data) according to the birth registration office [10]. Nearly 4 million electronic signatures are quite low considering Turkey's population.

	2018-2	2018-3	2018-4	2019-1	2019-2	Çeyrek Dönemlik Artış %
Elektronik İmza	2.992.301	3.092.381	3.262.833	3.452.307	3.592.786	4,1
Mobil İmza	518.160	535.740	554.486	569.760	580.992	2,0
TOPLAM	3.510.461	3.628.121	3.817.319	4.022.067	4.173.778	3,8

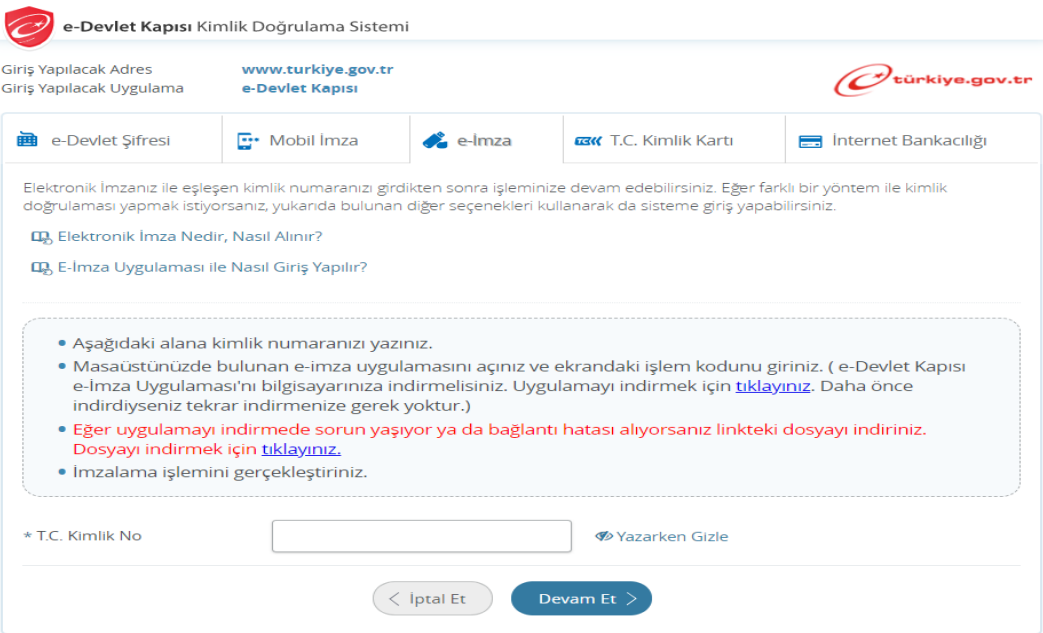
Figure 10 Total Electronic and Mobile Electronic Signature Certificate Numbers in Years [39]

In conclusion, secret password solutions are not considered as secure methods to authenticate users anymore under standard conditions, this method is also decrease the security level of the whole e-government system by being the weakest point and leaving the door open for possible threats.

3.1.2. Smart Card Based Methods

Smart card based identification is one of universally accepted methods based on two-factor authentication. The method itself contains two essential factors of two-factor authentication concept, possession and knowledge. While possession means actual ownership of EID token via smart cards, knowledge is reached by having the specific secret PIN/Password that protects access to the token [13].

After the preparation of the Electronic Signature Law No. 5070 [8], four companies started to serve as electronic signature certification authorities in Turkey [11]. The first applicable solution for producing electronic signatures adopted by these companies was smart card based solutions. These companies established their electronic signature system on the grounds of smart card methods in those days because there was no other e-signature solution structure accepted until the 2007, the introduction of mobile signatures. According to the data of second quarter of the year 2019; total number of produced electronic signatures is 4.1 Million, we see that 3.592.786 of them are electronic signature certificates and 580.992 of them are mobile signature certificates [39]. That being the case, smart card based solutions are still the most commonly used method for electronic signing in Turkey in 2019 [39]. We can see e-signature login via smart cards interface of Turkish e-government application below in the figure 11.



e-Devlet Kapısı Kimlik Doğrulama Sistemi

Giriş Yapılacak Adres www.turkiye.gov.tr
Giriş Yapılacak Uygulama [e-Devlet Kapısı](#)

[e-Devlet Şifresi](#) [Mobil İmza](#) [e-İmza](#) [T.C. Kimlik Kartı](#) [İnternet Bankacılığı](#)

Elektronik İmzanız ile eşleşen kimlik numaranızı girdikten sonra işlemimize devam edebilirsiniz. Eğer farklı bir yöntem ile kimlik doğrulaması yapmak istiyorsanız, yukarıda bulunan diğer seçenekleri kullanarak da sisteme giriş yapabilirsiniz.

[Elektronik İmza Nedir, Nasıl Alınır?](#)
[E-İmza Uygulaması ile Nasıl Giriş Yapılır?](#)

- Aşağıdaki alana kimlik numaranızı yazınız.
- Masaüstünüzde bulunan e-imza uygulamasını açınız ve ekrandaki işlem kodunu giriniz. (e-Devlet Kapısı e-İmza Uygulaması'nı bilgisayarınıza indirmelisiniz. Uygulamayı indirmek için [tıklayınız](#). Daha önce indirdiyse tekrar indirmenize gerek yoktur.)
- Eğer uygulamayı indirmede sorun yaşıyor ya da bağlantı hatası alıyorsanız [linkteki dosyayı indiriniz](#). Dosyayı indirmek için [tıklayınız](#).
- İmzalama işlemini gerçekleştiriniz.

* T.C. Kimlik No [Yazarken Gizle](#)

[İptal Et](#) [Devam Et](#)

Figure 11 Smart Card Based Login Page of Turkish E-Government Application [38]

The reasons of this method still being the most preferred method can be explained by these factors;

- Being the first method that has an adequate level of security
- People's habits
- Governments mostly supporting the application of old methods
- Insufficient demand for e-signature products in general

This situation applies not only to Turkey but also to the other countries' usecases as well. Two-Factor Authentication with Dongle Method seems to be very stable and still preferred method among countries according to the e-signature report of FORMIT Foundation [1].

If we look at the usecase of the smart card based methods, it can be referred as local signing usecase because user's keys are held on qualified signature creation devices in the form of smart card dongles. The general usecase and the identification steps can be seen in the figure 12.

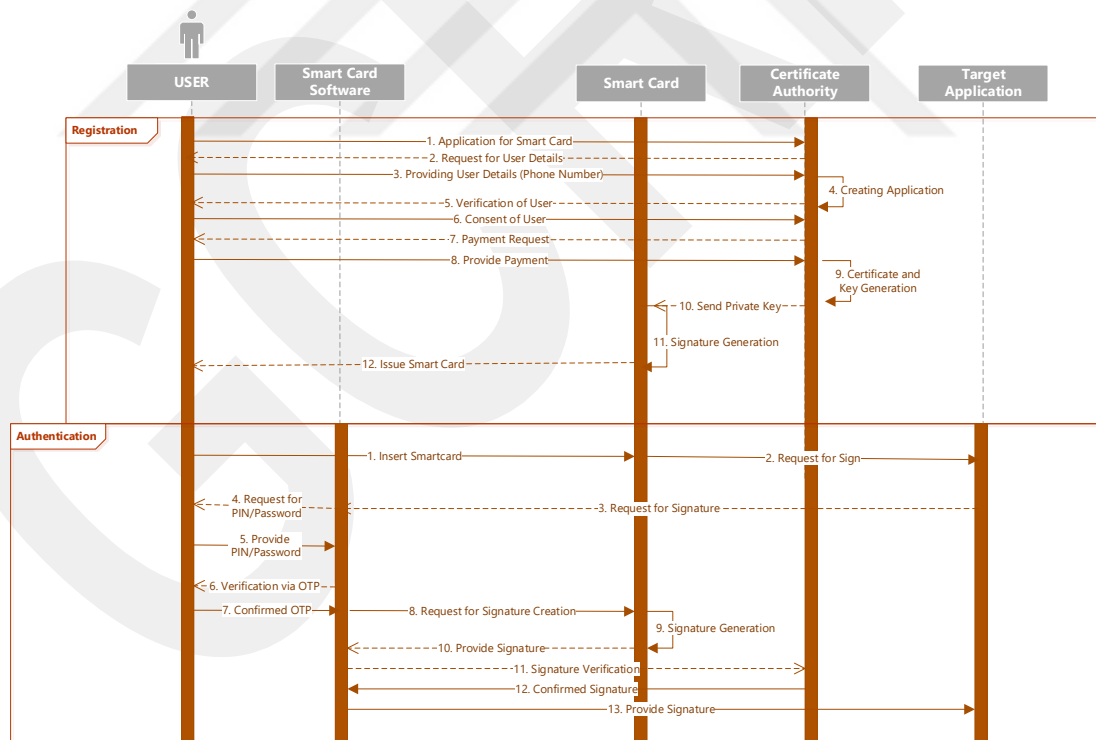


Figure 12 Smart-Card Based E-Signature Usecase in Turkey

In the registration face, a person can make an application to the Certification Authority through online, through phone or in person. After he/she provided the necessary information to prove that he/she is an actual legal person and gave his consent for the creation of his electronic signature; he/she provides payment for the service. After then certification authority completes generation of the unique electronic signature of the person and deliver the signature and signature creation device (dongle) that preserves the signature afterwards. Necessary information about usage of this e-signature including PIN/Password, access to necessary software, legal obligations, how to maintain the signature are given to the person at the end of the process. In this usecase, the preservation and security are met by the person himself and the total responsibility of securing the electronic signature belongs to that individual.

In the process of electronic signature usage, the person who wants to use his online identity should take some necessary steps beforehand. First of all the method requires a computer since dongle preserves the smart card. Then person should download the necessary software(s) into computer in order to execute the electronic signature creation correctly. After completing the steps without any confusion, user inserts the dongle (smart card) to the computer and starts the signing process to a receiver party. The signature creation process first needs the user's PIN/Password to initiate the signing. This is referred as knowledge factor in two-factor authentication schemes. Then an OTP (one time password) created through the software and it is send to the users' mobile phone. This step is increasing the security of the case which the signature is not under the possession of its user (stolen, lost etc.) while it also helps the fulfillment of possession factor in two-factor authentication schemes. After user verified the correct OTP message to the signature software on computer, the electronic signature is created.

Although Turkish smart card based signature creation usecase has its advantages such as adequate level of security, accordance with Turkish law of electronic signing etc., it has also disadvantages, which affects user's utilization. These disadvantages can also be seen as the reasons why this method does not spread to the desired degree in Turkey. In the study of Kabasakal in 2017 [9], it was mentioned there as well that widespread use of e-signature could not reach the expected levels due to the inability to establish e-government and e-institutions on time, high costs and insecurity in new technologies in spite of the 1999 Electronic Signature Law and secondary regulations were enacted in our country in time [9]. In 2019, some of these disadvantages still present are;

Low Level of Usability

Alongside of the adequate level of security of smart card based authentication, smart card based solutions found to be lack an appropriate level of usability. The main disadvantage is explained as *“Unfortunately, smart card based solutions usually lack an appropriate level of usability, as they require users to obtain, install, and use an appropriate card-reading device in combination with the associated software”* in studies of Rath et al. [16] [15].

Dependency to Hardware

Electronic signatures are preserved at smart cards in dongles in this solution. This situation causes the liabilities of carrying the signature creation device around all the time and dependency to a computer.

Lack of Common E-Signature Software and Hardware

There are currently six electronic signature certification authorities working in Turkey actively in 2019 [11]. In these providers' processes, hardware module types preserving electronic signatures and signature software are all different from each other. Different software's' interfaces and device types can be seen in figure 13,14,15,16 and 17. It leads to a great confusion on the end user side if they has to manage more than one electronic signature in their daily lives or if they need to change their certification authority for any reason. People encounter with different software and different interfaces each time since there is no common interface for them.

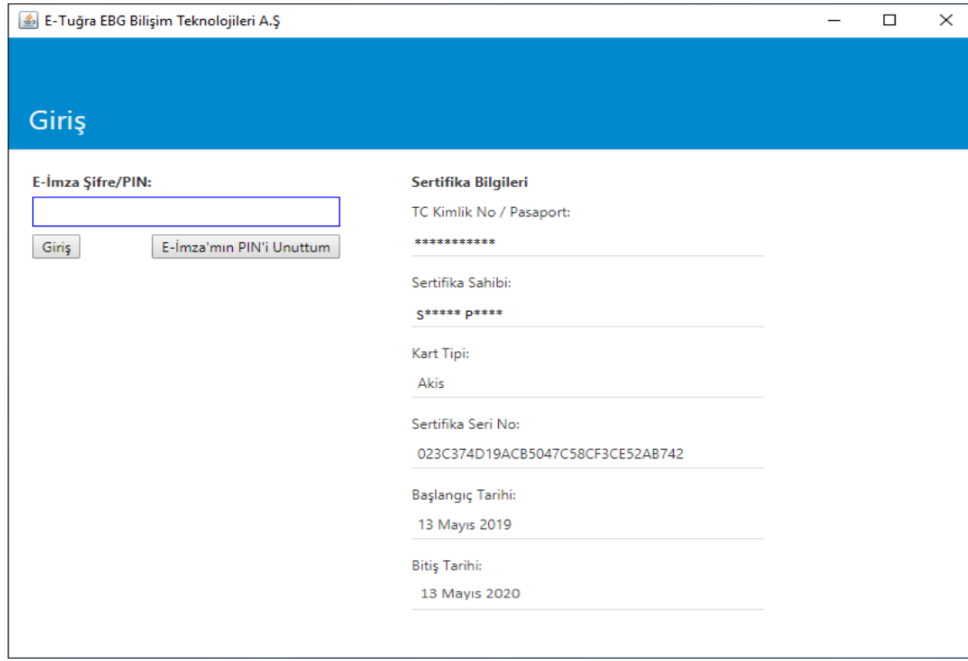


Figure 13 Interface of the Software of E-Tuğra Information Technologies and Services Inc. [40]

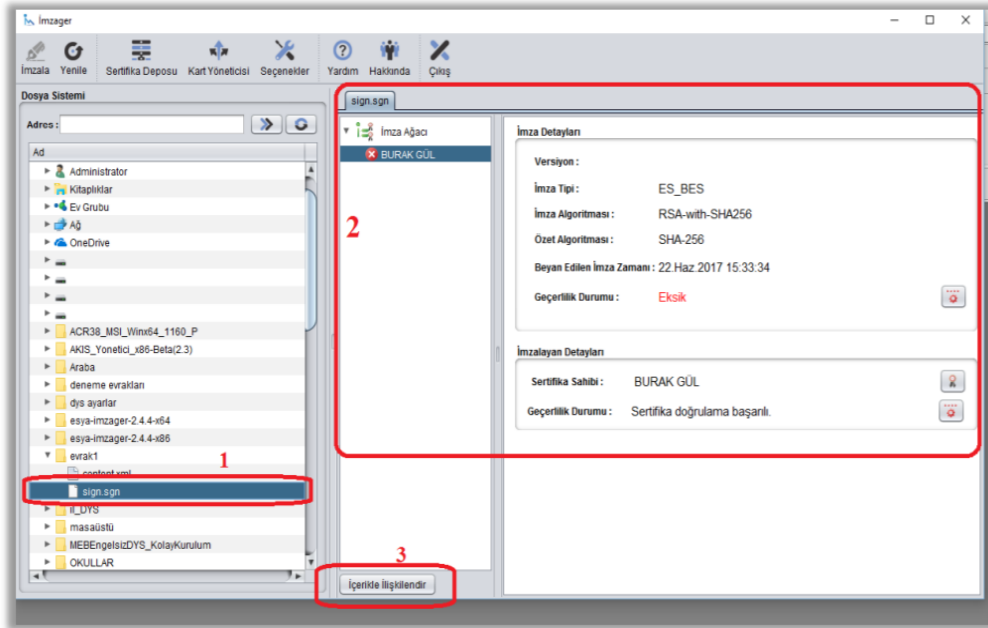


Figure 14 Interface of the Software of Scientific and Technological Research Council of Turkey [41]



Figure 15 Interface of the Software of TURKTRUST Information Security Services Inc. [42]



Figure 16 Dongles of Scientific and Technological Research Council of Turkey [41]



Figure 17 Dongles of TURKTRUST Information Security Services Inc. [42]

Different Applications Operating with E-Signature Service Providers

In institutions, public or private, the selection of the e-signature depends on the agreement between e-signature service providers and institutions in Turkey. Number of Electronic signature authority is six however, there are many other individual private companies that provides different software processing the electronic signatures and performs e-signature integration to the sector specific applications. They are called e-signature service providers. These are mostly sector specific companies and solutions, which provides an easy integration of e-signatures and enable users from these sectors, use electronic signatures from their own system. Institutions generally do not have specific electronic signature software of their own so that they purchase the software from these private companies.

For example, there is an obligation of using an electronic signature from a specific certification authority, TUBİTAK-UEKAE (Kamu Sertifikasyon Merkezi), for the employees of Turkish public system in Turkey. Therefore, different signatures purchased by other certification authorities are not valid in public office operations.

Another example is the situation in the hospitals in Turkey; doctors have to use electronic prescription after the notice of directorate of social security organization since 2018. The HIS (Hospital Information System) software are integrated with different private e-signature providers' systems to implement electronic signature solutions. Therefore, the certification authority whose e-signature provider integrated its system provides e-signatures of this hospital. This situation results in, doctors experiencing compatibility problems with their e-signatures when a doctor transferred

to another hospital or among doctors having electronic signatures from different certification authority. It causes low usability for the users.

Economical Disadvantages

There are six certification authorities for electronic signatures in Turkey; there is a market of it. There is high prices for electronic signatures because it requires advanced technology and it provides a qualified security service, which is important. These providers provides different services to its customers to get ahead of one another. Based upon these services such as fast delivery, fast signature creation, nearby offices to provide accessibility, end user support system; they can also request different prices for an electronic signature. These high prices are another reason of low demand for electronic signatures from individuals and institutions. Except from the institutions, which electronic signatures are mandatory, institutions and individuals do not want to pay any money to electronic signatures unless they have to.

3.1.3. Mobile Methods

Mobile electronic signature concept is defined as electronic signature generation either on a mobile phone or on a SIM card in a mobile phone. Simply, the cryptographic operations are performed on special SIM cards instead of smart cards. Since these SIM cards are able to handle cryptographic operations as well as they perform their main network operations, they can be counted as smart cards. The e-signature technology offered via SIM card allows users to use e-signature in any environment and at any time without the need for an additional card or card reader.

According to the researches performed in 2007, two different concepts of mobile signature are introduced; Client Based Mobile Electronic Signature and Server-Based Mobile Electronic Signature [9]. First of them, Server-Based Mobile Electronic Signature, is defined as signatures created by a certification authority on a secure server on behalf of individuals [9]. The second method of mobile signature was Client Based Mobile Electronic Signature. The advantage of the client based method was that it provided a legal basis for authentication of the user at the time. In contrast to the server-based method, this method was suitable with the Article 4 (b) of the Electronic Signature Law No. 5070 [8], "*Secure e-signature; It should only be created with a secure e-signature creation tool at the discretion of the signatory*" [9] and

paragraph (c) of Part 2 of the Directive *"in order to obtain a secure e-signature, the signature must be created in such a way that the signatory remains under his or her own private control"* [9].

After all, the institutions and government adopt the idea behind the client based method. With the introduction of Communiqué Amending the Communiqué on the Processes and Technical Criteria Regarding Electronic Signature [8] which is published in the official gazette dated 26/06/2008 and numbered 26918, necessary legal grounds for mobile solution is met. Necessary agreements are completed with GSM operators and certification authorities since GSM operators were responsible for generating smart SIM Cards and certification authorities were responsible for generating secure signature creation devices and providing the mobile electronic signature certificates.

The application of this method requires two parties' collaboration, certification authorities and the GSM operators due to its nature. The collaboration between these parties is ensured by mobile signature service providers, which are third party companies. Firstly, the user, who has a mobile phone that contains special smart SIM card in it, sends a request for the service provider of the target site aiming to authenticate himself/herself. This request transferred to the mobile (GSM) operator and signing request with necessary signing information is send to the user's mobile phone. It ask for user's secret signing PIN/Password to start the signing operation ad after the PIN/Password is provided by the user, signing operation is completed on the mobile device. Then signed data is send to the mobile operator who transmits this signed data to service provider of the target site. The last step of the process is verification of the signature. To do that, signed data is send to the certification authority by service provider. After the certification authority verifies the signature, authentication of the user is complete. The representation of the usecase is given in the figure 18 below.

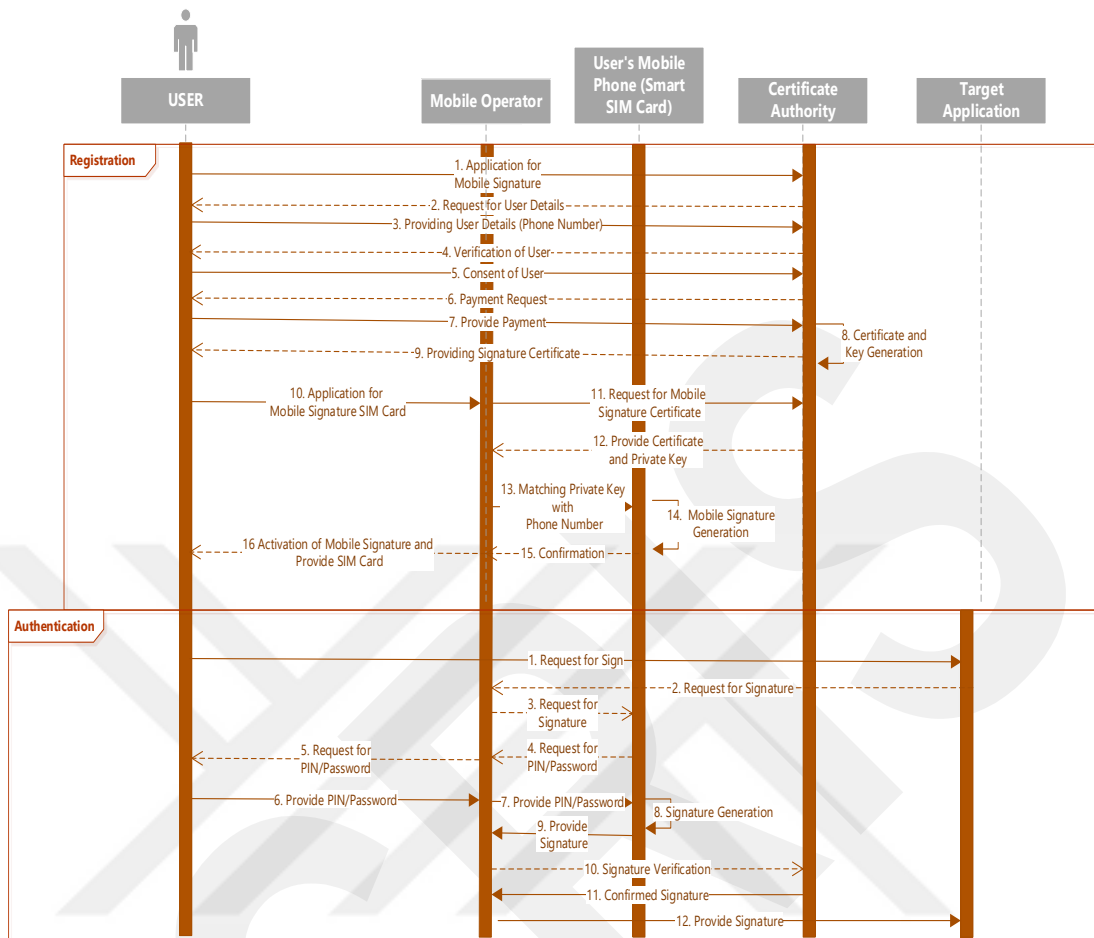


Figure 18 SIM Card Based Mobile Signature Usecases in Turkey

In 2019, three certification authority continue to provide mobile e-signature certificates in collaboration with three telecom companies. These companies can be seen in table 3.

After the necessary legal grounds for mobile e-signature solution is prepared in Turkey, e-government application integrated mobile e-signature solution into its structure since it is legitimized under the eyes of government. The interface of the mobile e-signature login page in the e-government application is given in the figure 19.





 e-Devlet Şifresi	 Mobil İmza	 e-İmza	 T.C. Kimlik Kartı	 İnternet Bankacılığı
<p>Cep telefonunuz ve hattınıza kayıtlı mobil imzanız ile kimliğiniz doğrulandıktan sonra işleminize kaldığınız yerden devam edebilirsiniz. Eğer farklı bir yöntem ile kimlik doğrulaması yapmak istiyorsanız, yukarıda bulunan diğer seçenekleri kullanarak da sisteme giriş yapabilirsiniz. Mobil İmza Nedir, Nasıl Alınır?</p>				
* T.C. Kimlik No	<input type="text"/>	Yazarken Gizle		
* GSM Numaranız	<input type="text"/>	Mobil imzanızın tanımlı olduğu, 10 haneli cep telefonu numaranızı giriniz. Örn: 5XXXXXXXX		
* GSM Operatörünüz	<input type="radio"/> Türk Telekom	<input type="radio"/> Turkcell	<input type="radio"/> Vodafone	
Hattınızın hizmet aldığı GSM operatörünü seçiniz.				
<input type="button" value="İptal Et"/>		<input type="button" value="Devam Et"/>		

Figure 19 Mobile Electronic Signature Login Page of Turkish E-Government Application [38]

When Turkish government started their e-government studies, a mobile environment for e-government, m-Government application, is also aimed in the vision [32]. After all, enabling citizens to access the required information at anytime and anywhere without time and place limitations was an important angle in the project [32]. Mobile Government applications aim to provide the necessary information to the citizens with widespread telephone support even in the absence of computers. The e-Government Gateway mobile application (m-Government) has been designed and currently Turkish citizens can use the m-Government application by downloading it from Apple and Android Stores free of charge [32]. Signing into this mobile application is only possible via mobile signature or e-Government password [32]. We can see the interface of the mobile government application in the figure 20 below;



Figure 20 Mobile Application Login Page of Turkish E-Government [38]

Although the legal and systematic basis are provided for this solution to work, the concept of mobile electronic signature has not seen much interest in Turkey. According to 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 [39].

3.1.4. National ID Cards

The national ID card concept was always a popular concept among countries. Austria [33], Estonia [34], Belgium [35] and Spain [36] are some of first countries that have issued personalized smart cards for their citizens [43] [15].

In Turkey, the basis for unique identities is constituted between the years 2000 and 2002 with a nationwide identity project called The Central Civil Registration System (MERNIS) [37]. With the MERNIS project, it is aimed to share citizen information in a safe and fast manner and to increase the speed and efficiency in the service provided to the citizen [37]. Today MERNIS project continue to serve the citizens of Turkey as

a centralized databank of ID's, providing information services in electronic environment and statistical data. As a result of this project, unique identities for citizens are provided. However, as e-Government technologies developed over the years, strong authentication methods are became a need [37]. As a result of this need, the social security card project conducted by Scientific and Technological Research Council of Turkey (TUBİTAK-UEKAE) and Social Security Institution was transformed into national ID card project [37]. First studies regarding the citizen card concept are started with national ID card project in the years 2008 [37]. Citizen cards officially started to be distributed to citizens all over the country through general directorate of population and citizenship affairs at the beginning of 2017 [10]. Citizen cards continue to be distributed in 2019 and the information of number reaching 37 Million (nearly half of the 82 million population in Turkey) was shared by the e-population union of public employees in 2019 [10].

The Turkish national citizenship card, which is actually a personalized smart card, enables ID verification with different credentials such as visual security elements, pin code and biometric data (fingerprint) [44]. The biometric data on the card is held exclusively and not stored in a central database [32]. Cards are designed in credit card size and international norms in terms of ease of transport, they are made of high-strength material suitable for long-term use [10]. Turkey Identity Card has a validity period of 10 years and the design of the card supports the most advanced security elements to prevent unauthorized person to reproduce the card or modify the information on the card [10].

The start is given for the applications of the national ID cards on 14 March 2016 in Kırıkkale city of Turkey [10]. Further application began in ten pilot cities in October 2016 after that the new Turkish national ID cards were available for all citizens through the whole country since 2017. As of 2017, every citizen has to get his/her national ID card until 2023 [10]. Besides the above-mentioned properties of the new national eID cards, it also includes a built-in e-signature feature so that the owner can use it to access to e-Government services ones he/she gets the e-signature certificate [32]. The usecase for e-signature usage through the national ID cards is given in figure 21 below;

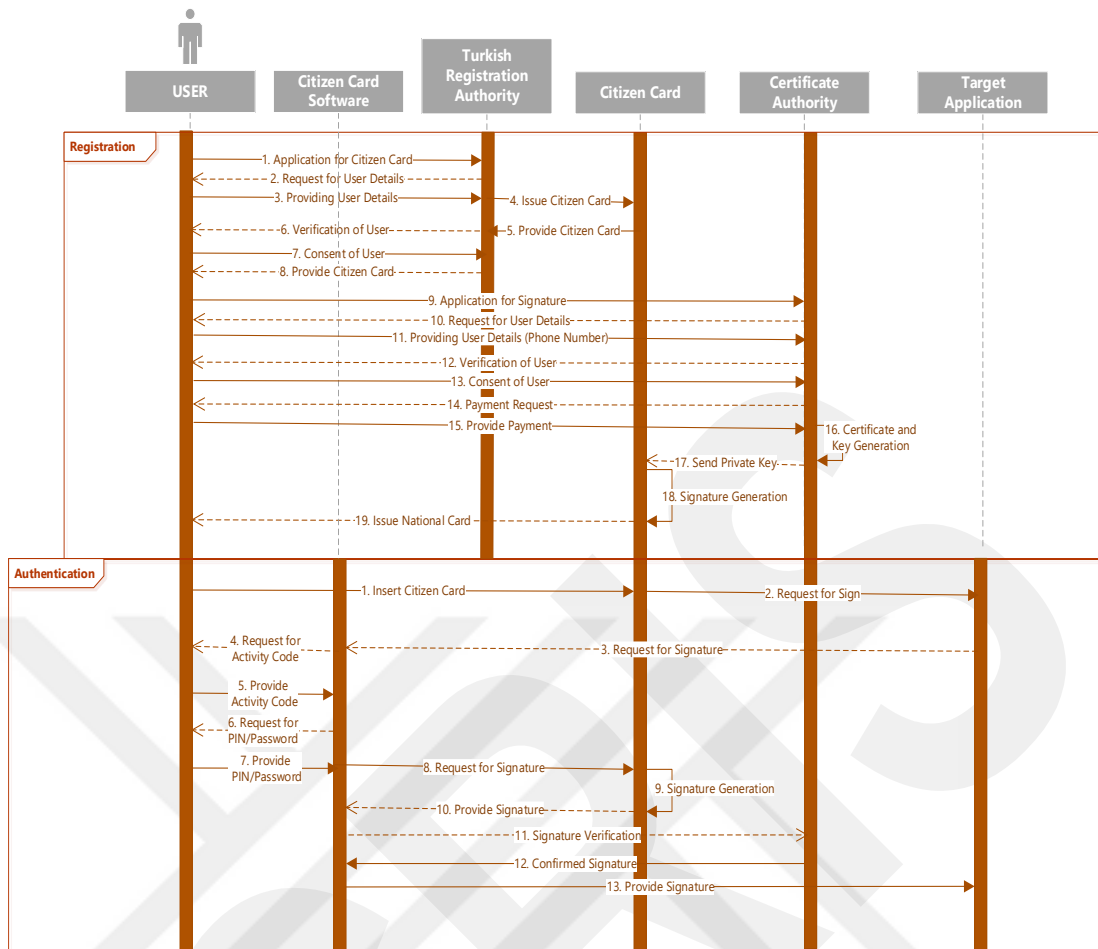


Figure 21 National ID Card Based e-Signature Usecase in Turkey

General directorate of population and citizenship affairs provides citizen cards since 2017. Firstly, citizens should apply to get their new ID card and hand over their old ID card. Necessary information (biometric data, biometric photo, signature etc.) are taken from the user to construct the new ID card and ID card creation process is started. After the application of Republic of Turkey national card, personalized ID card will be delivered to the user's specified address by mail. E-signature within the ID card is not provided with the card itself beforehand. ID cards supports the usage of e-Signature, however it is up to the user to add an e-signature to his/her ID card. The user needs to get his/her national ID card and apply to a certification authority in order to add an e-signature to his/her national ID cards.

In the electronic usage process, national ID cards requires a card-reading machine and a special national card software. After inserting the card to the card reader, a request is made to the target site. Target site is the produce an activity code for the

request. User needs to enter this activity code and his/her password/PIN to the national card software to start the signing process. If the given information is true, signature is generated inside the national card, which is connected to the computer at that moment, and the signature is delivered to the target site by national card software. An example interface for the national card usage belonging to the e-government application is given in figure 22.

e-Devlet Kapısı Kimlik Doğrulama Sistemi

Giriş Yapılacak Adres www.turkiye.gov.tr
Giriş Yapılacak Uygulama [e-Devlet Kapısı](#)

[turkiye.gov.tr](#)

e-Devlet Şifresi Mobil İmza e-İmza T.C. Kimlik Kartı İnternet Bankacılığı

Kimlik numaranızı girdikten sonra işleminize devam edebilirsiniz. Eğer farklı bir yöntem ile kimlik doğrulaması yapmak istiyorsanız, yukarıda bulunan diğer seçenekleri kullanarak da sisteme giriş yapabilirsiniz. [T.C. Kimlik Kartı Nedir?](#)

- Aşağıdaki alana kimlik numaranızı yazınız.
- Masaüstünüzde bulunan Kimlik Kartı uygulamasını açınız ve ekrandaki işlem kodunu giriniz. (e-Devlet Kapısı Kimlik Kartı Uygulaması'nı bilgisayarınıza indirmelisiniz. Uygulamayı indirmek için [tıklayınız](#). Daha önce indirdiyse tekrar indirmenize gerek yoktur.)
- Kimlik kartı doğrulama işlemini gerçekleştiriniz.

* T.C. Kimlik No Yazarken Gizle

[İptal Et](#) [Devam Et](#)

© 2019, Ankara - Tüm Hakları Saklıdır Gizlilik ve Güvenlik Hızlı Çözüm Merkezi

Figure 22 National ID Card Login Page of Turkish E-Government Application [38]

Although national ID cards have started to be distributed to the citizens since 2017 in Turkey, legal framework constituted for this transformation is still insufficient [45]. National eID concept is only mentioned in Article 41 of Law 5490 on Civil Registry Services [45] and because of its nature and differences from traditional printed IDs, a specific legal framework is required according to the international Law Office's report [45].

While forming a technical basis for the usage of national citizen cards, legal framework of the solution should also be considered. However, in the current situation, Turkey has only the Electronic Signature Law No. 5070 covering only the electronic signatures [8]. The lack of a clear legal landscape for national eIDs was also a problem within the European Union since Directive (1999/93/EC) covers electronic

signatures only [2]; however, eIDAS regulation covers all types of e-signatures and eID schemes since 2016, presenting a solution to these problems [6].

3.1.5. oAuth

The oAuth protocol is an open protocol that allows Web, Mobile and Desktop applications to authorize applications in a simple, standardized way [46]. It does not offer an e-signature technology in its body. However, with its easy implementation, oAuth has simplified the secure access to the protected data that normally with limited access [46]. Today, most social media applications (Facebook, Google etc.) support the oAuth protocol. The fact that the websites offer a login option to their users with their Facebook or Google accounts provides great convenience to these users.

Today, banks are the only institutions providing legal online identities of Turkish citizens which e-Government application recognizes. Supporting that idea, Turkish citizens can log into e-government website via their bank accounts [38]. Currently 20 Banks provides oAuth mechanism to integrate their system with the e-government services. We can see the login page of Turkish e-government application supporting oAuth mechanism in figure 23.

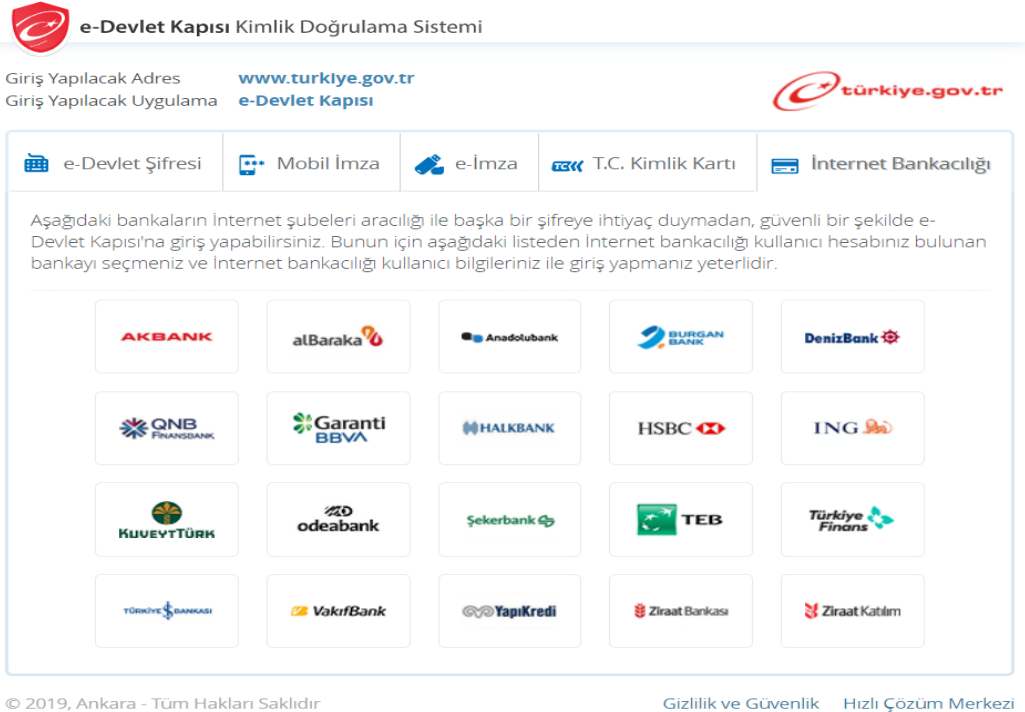


Figure 23 oAuth Login Page of Turkish E-Government Application [38]

Citizens first open the web application of the e-government. They choose the oAuth option to login. Then they have to choose the bank which they have their legal bank accounts on. After choosing the bank, user is directed to the login page of the chosen bank. After user provided his correct login information (usually customer number/ ID number and password), information is checked by the bank. If the given information is true, his authentication conformation is transmitted to the e-government application. Therefore, secure access to e-government application of the user is provided. The functioning of oAuth mechanism between banks and the other applications (such as e-government) in Turkey given below;

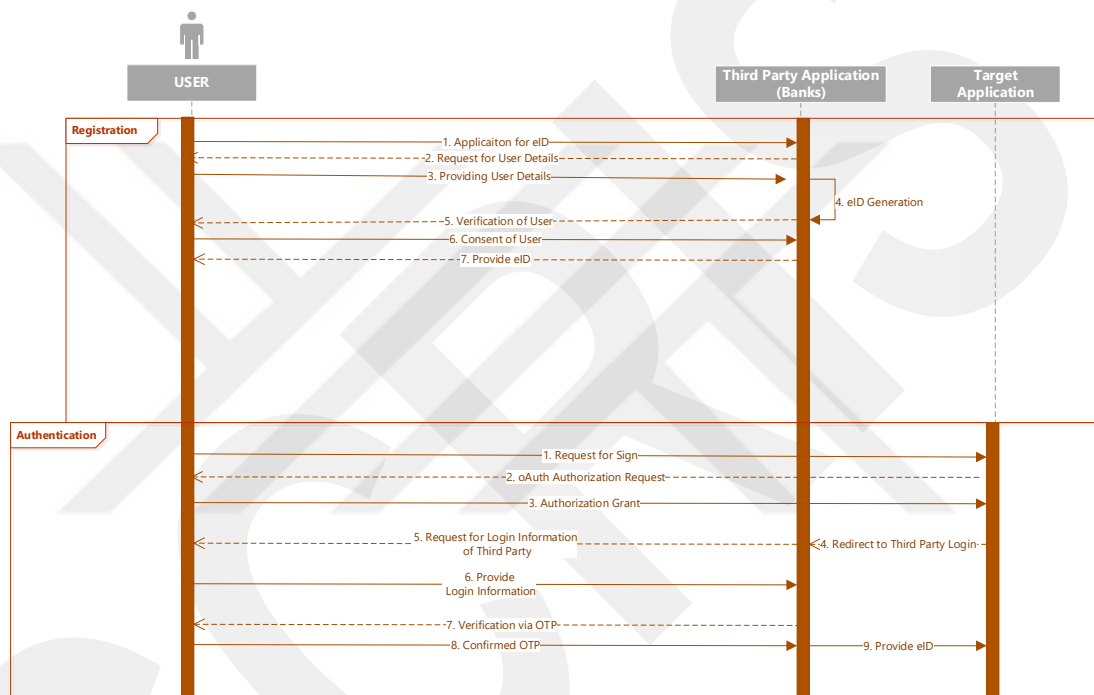


Figure 24 OAuth Mechanism via Banks in Turkey

Method itself depends on the banks' security systems. From the point of e-government application, banks are legal and secure institutions and their authentication mechanisms are trusted. Thanks to this method, user can login both bank's account and e-government account using the same password via the same interface with the same usecase. It sure increases usability for users, however this authentication process can not be seen as a production of qualified electronic signature method since there are no certification authority in the process.

Besides that, the online identities created by the banks are not verifiable by a single point they are not unique identities. A person can have numerous different online

identity associated with the banks in theory. Banks manages these identities under their own databases. Since these identities of the person do not tied to a single certification authority, they are not counted as qualified electronic signatures and verification of these identities is handled by the banks themselves. This situation results in, applications which want to integrate an oAuth mechanism with banks should work with all of the banks separately. It produces a lot of work for the institutions to provide an integration with every bank. This solution is realized in the e-government system so far, even they could integrate their system only with the 20 banks.

There are currently 47 banks actively working in the Turkey [47]. This solution does not cover banks and customers other than 20 banks integrated into the system. To provide an integration technology with e-government system requires certain security level and efforts for these banks. Consequently, the customers of not integrated banks can not benefit from this method.

Since there are still different usecases and domain specific solutions used in Turkey, there is no unified system achieved so far. A unified system is important for cross-border authentication as well as it contributes to the target of more sustainable and usable system.

CHAPTER 4

4. A SERVER-BASED E-SIGNATURE METHODOLOGY THAT CAN IMPROVE THE E-SIGNING PROCESSES IN TURKEY

4.1. Server-Based E-Signing Methodology

Over the years, different structures are introduced to improve eID and electronic signatures concepts as it mentioned in section two. Among these structures, server-based approaches have been increasingly followed. Orthacker et al.'s server-based method relies on a concept that cryptographic operations can be handled in hardware security modules (HSMs) instead of users' local devices such as SIM cards or smart cards [19]. However, server-based signatures were in general considered not to fulfill the requirements of advanced electronic signatures according to the Directive 1999/93/EC [19]. Before the eIDAS regulation enter into force, according to the advanced electronic signature definition of the Directive 1999/93/EC, private keys of the users must be maintained under users' sole control [2]. Since, the signature keys are maintained under a secure server instead of users' device in the structure of server-based e-signing, it was claimed that the signatory gives away control over the signature-creation data [19]. However with the introduction of the eIDAS regulation, server-based signatures with HSMs are legally supported too.

Despite this legal obstacle, Austria was one of the exemplary countries where server-based eID concept is implemented and in use for several years countrywide. Austria has made the necessary legal arrangements in its electronic signature law allowing the usage of server-based methods in the country in addition to the main national ID card solution [19].

In Turkey, there have been no attempt to implement any national server-based eID structure so far. As it mentioned in the third section, current eID and electronic signing

methods depend on the structures where one's signature keys are kept in sole discretion. In all of the methods (smart card method, mobile/SIM card method, national ID card method) signature keys and cryptographic operations are performed in smart cards or SIM cards. In order to achieve an international and more usable eID structure in Turkey, server-based eID solutions and especially Austrian usecase are examined.

4.2. Austrian eID Ecosystem

Austria's eID ecosystem is considered technology-agnostic due to its capability of integrating different concepts such as HSMs, mobile solutions, cross-border usecases etc.. In the eID scheme of Austria, current implementations in use are based on National ID smart cards and server-based mobile signatures [13]. At first, Austria established citizen cards for the use of digital e-Government applications [13] together with the corresponding software (MOCCA Software) to handle citizen card functions [48]. After that, with a public-private partnership, server-based mobile phone signature solution and its technical infrastructure are developed by Egiz (E-Government Innovation Center) a joint initiative of Federal Chancellery Austria, Graz University of Technology and certification service provider A-Trust [48]. Austrian eID solution is a combination of National ID Smart Card and server-based mobile signature methods. eID Ecosystem in Austria is shown in the figure 25.

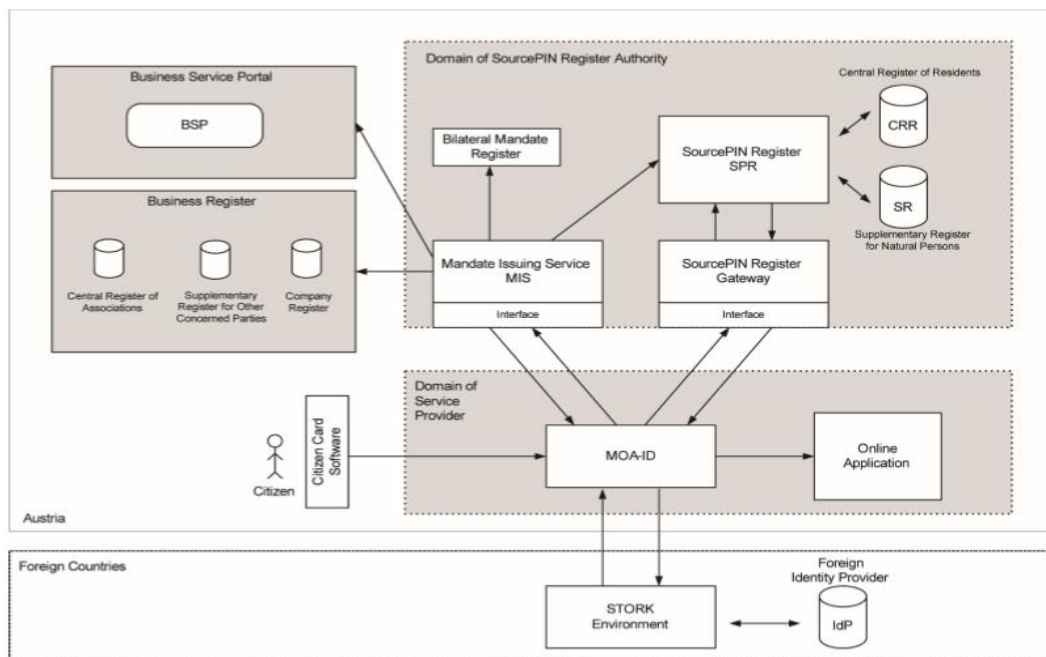


Figure 25 eID Ecosystem in Austria [13]

A central element called MOA-ID and several other components provides secure authentication of citizens according to the Austrian eID concept [13] [15]. MOA-ID is actually provides a security layer to handle connections between e-Government applications and Citizen Card functionality. This way, citizen card applications do not need to integrate themselves with different e-government applications since all e-government services can be accessed through a common interface. Also with the separation of e-signature function and eID (e-government) function, MOA-ID improves the security measures of the general system. MOA-ID also has a template providing a selection page for preferred Citizen Card configurations for the end users as it can be seen in figure 26 [48]. With this functionality, MOA-ID supports both citizen card concept and server-based mobile signature concept [48].



Figure 26 MOA-ID Template [48]

In the Austrian eID scheme, Citizen Card Software also play an important role acting as middleware between citizens and MOA-ID in the Austrian e-Government infrastructure [16]. MOCCA (Modular Open Citizen Card Architecture) software is an example of a citizen card software, which developed by EGIZ (e-Government Innovation Centre) in Austria [48]. The modules of the MOCCA software and Mobile Phone Signature architectures are explained in detail during usability evaluation study conducted by Zefferer [16]. The structures of local and online sub-solutions of the MOCCA software are given by Zefferer in his study as it can be seen in the below figures 27 and 28.

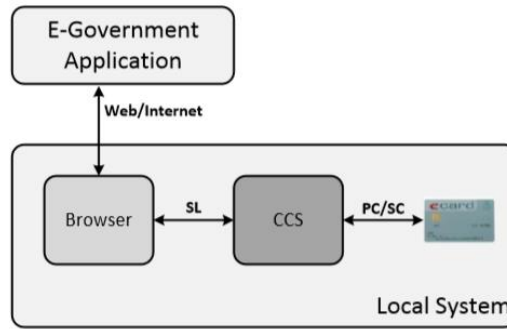


Figure 27 MOCCA Local Architecture [16]

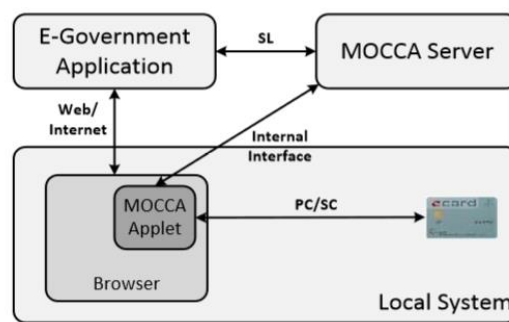


Figure 28 MOCCA Online Architecture [16]

Another citizen card implementation is named mobile phone signature concept which is a server-based e-signature methodology [16].

4.2.1. Austrian Server-Based Signatures (Mobile Phone Signature)

Mobile phone signature function, which is a server-based e-signature methodology, is provided by certification service provider A-Trust [48]. Austrian mobile phone signature concept depends on the basis of two-factor authentication (knowledge & possession) scheme. Signature-creation data (cryptographic keys) are kept at secure HSM devices but controlled by the signatory himself/herself [48] [49]. Since HSM devices are accepted as qualified signature creation devices, mobile phone signature concept is now compatible with eIDAS too [6].

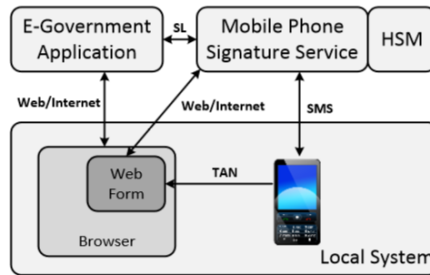


Figure 29 Austrian Mobile Phone Signature Architecture [16]

As it can be seen in the above figure 29, in an eID structure formed in this manner, several other components are necessary for the mobile phone signature service [16]. Mobile Phone Signature Service component is a server side element of the solution having five components in itself; a web interface for communication between the user and the server, an SMS gateway for sending SMS to the mobile phones, Hardware Security Module (HSM), a database containing signature creation data of the user in an encrypted form and a person register [16]. The Mobile Phone Signature Service also integrates with the MOA-ID central component of the Austrian eID structure while reaching the online applications. Web interfaces of the Mobile Phone Signature solution provided by A-SIT are given in the figure 30.

Figure 30 Mobile Phone Signature Interfaces provided by A-SIT [48]

Server-Based Mobile Phone Signature concept established on an architecture supported through open source building blocks in the Austrian eID environment in accordance with the STORK 2.0 project [49]. According to the ITU resources, Austrian mobile ID solution gains approximately thousand new users per day in Austria in the year 2016 [49]. Mobile ID is used in about 300 online services and there are about 700 thousand active mobile eIDs in comparison to 120 thousand active smartcards

[49]. Key success factors considered to be; no additional hardware usage (Operable in any browser on any Operating System), no SIM card change needed through server-based solution, easy activation for citizens and low development costs (no cost for citizens) [49].

4.2.2. A Modular Approach to Austrian Server-Based Signatures

According to the FORMIT Foundation's report, lack of clarity in terms of implementation is one of the weakness of Directive 1999/93/EC [1]. This weakness causes different usecases as well as different eID structures across countries. Most of the server-based eID and e-signature solutions that have been introduced suffered from this weakness and Austria's server-based eID approach is no different [15]. In the study of Rath et al., they propose "a modular and flexible concept for mobile eID and e-signature solutions" to overcome this limitation [15].

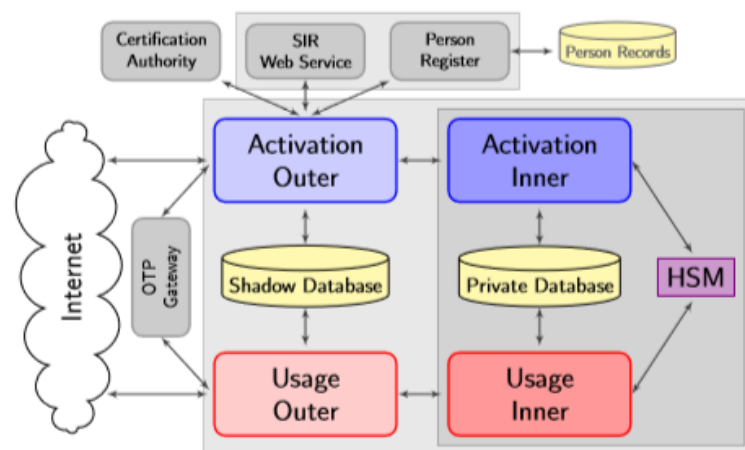


Figure 31 Overview of Components of Rath et al.'s Method [15]

As it seen in the above figure 31, the design of the Rath et al.'s work allows external parties to work with outer part of the databases while inner database stays secure at the same time [15]. Proposed concept of Rath et al. is a critical work for this research because of its flexibility and its compatibility to different use cases [15]. In their study, they have designed their proposed solution based upon server-based mobile eID and e-signature architecture proposed by Orthacker et al.. [19] [15]. Architecture is composed of four core components (Activation Outer, Activation Inner, Usage Outer,

and Usage Inner) and the split between inner and outer components provides extra security in case of outer part be compromised [15]. Data protection in the inner part is provided by hardware security modules (HSM) implemented centrally [15]. The connection between inner and the outer part is protected by an encrypted channel [15].

The outer part of the structure also may serve as a central point for certification authorities to combine their databases as we can see. Since Turkey has six certification authority currently active and key-generation operations are handled by these authorities for the present, this solution might help making it possible for Turkey to implement a server-based eID structure with some modifications.

Rath et al.'s proposed solution for Austrian mobile phone signature is consist of registration, activation and usage processes [15]. This processes are further examined in order to see whether they are applicable to the existing infrastructure of Turkey.

Registration Process

Registration process is an important process that, necessary data is collected from the users in order to identify them correctly. The basic goal of the registration process is the creation of an identity record identifying the specific user.

Rath et al.'s method is designed to support different types of registration [15]. In order to provide a flexible setup of the registration process, registration via private-sector domain is supported as well as official government domains [15]. They called the created identity records as Standard Identification Record (SIR) in their solution [15]. A record is used to identify the user and provide this user with basic access to the solution [15]. They introduce three different registration types in their study but they specified that basis of the solution supports different types of registration as well [15]. Their proposed registration types were; registration via registration officer, self-registration and registration via trusted organization [15]. The representation of these three methods can be seen in the below figure 32.

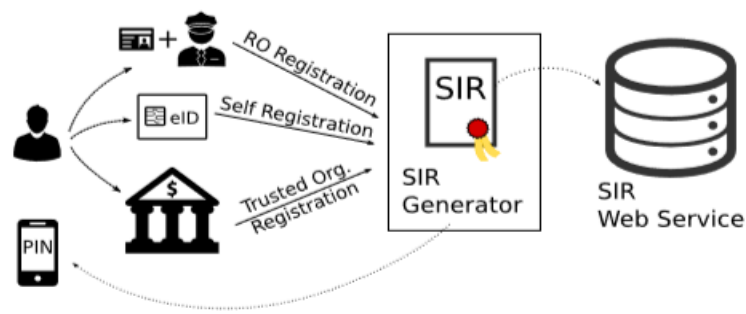


Figure 32 Registration Process of Austrian Mobile Signature Proposed by Rath et al.

[15]

Registration via registration officer supports face-to-face verification of a user. This verification is performed via official IDs, a passport or a driving license [15]. Officer manually registers the users in the system with their user specific data [15]. Self-registration option targets the users with existing eIDs [15]. An online environment is provided in the solution verifying the user's identity and enabling users to complete the registration on their own [15]. Lastly the registration via trusted organization option is covers the private-sector domains [15]. Existing identification data from legal organizations such as bank institutes or universities can be used to register new users [15]. After registration is completed, the SIR records are kept in person register component in a standardized way [15].

Activation Process

Second part of the Rath et al.'s method is the activation process. After successful registration to the proposed system and valid SIR (Standard Identification Record) for the user is created, users have to activate their accounts and create an eID for themselves [15]. Users are able to create multiple eIDs [15]. In the proposed usecase, users login to the system, fill an activation form and provide a phone number and unique secret password for each eID they want to create [15]. These two information is important for the two-factor authentication concept. Phone number is used to satisfy possession factor while secret password is used to satisfy knowledge factor. An important detail here is that users has to prove possession of the given mobile phone number [15]. This requirement is met by one-time password send to the users phone as we see in the below figure 33.

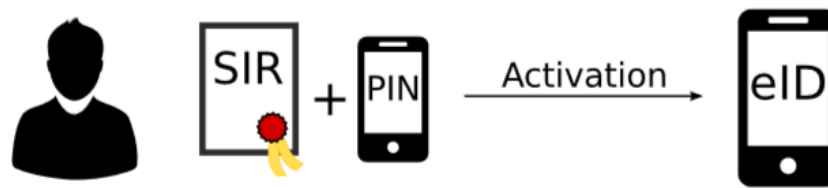


Figure 33 Activation Process of Austrian Mobile Signature Proposed by Rath et al.

[15]

In the activation process, public and private keys of the eID is created at HSM while a certificate for that user is also created by the help of certification authority [15]. After an eID is created for the user, it contains specific phone number and secret password information besides the personal information of that user transferred from person register [15]. In the proposed method, person register is defined as “*component that connects to an external database containing potential users of the service*” [15]. It can connect to either an existing official database like general directorate of population and citizenship affairs’ database or, an existing domain-specific database like banks’ databases. At the end of the process, created eID and public key are together signed by the person register. This signed structure, keys and the certificate information are all maintained in the solution’s database. An important gain of this solution is explained as the separation of the eID and e-signature functionalities assuring the users’ privacy [15].

Usage Process

Once the SIR (Standard Identification Record) and eIDs for the users are activated, users are ready to use their eIDs to authenticate themselves. If a signature creation is requested, firstly the user is asked for a secret PIN/Password to unlock the private key [15]. At this stage the signature-creation data is still protected by HSM [15]. After that an SMS containing OTP (One Time Password) is sent to the user’s registered mobile phone [15]. If the user provides this authorization code correctly on the server signature’s web interface, the requested signature is created [15]. The representations and the sample interfaces of the processes are shown in the below figures 34 and 35. The main advantage of the mobile signatures are considered as the central HSM device usage, which renders smart cards unnecessary [16] [15].

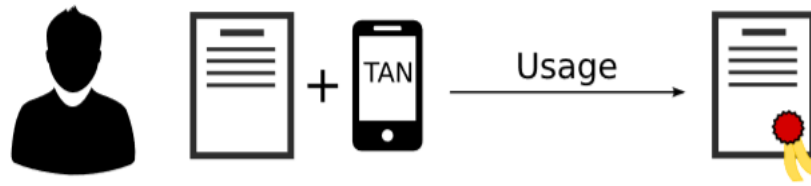


Figure 34 Usage Process of Austrian Mobile Signature Proposed by Rath et al. [15]

The figure shows two screenshots of the MOCCA mobile application interface. The left screenshot displays the login screen with fields for 'Telephone Number' and 'Signature Password', and a 'Login' button. The right screenshot displays the 'View Signature data' screen with a 'Reference value' of '42pMNpuKFp', a 'TAN' input field, and buttons for 'resend SMS' and 'Sign'.

Figure 35 Interface of the Usage Process of Rath et al. [15]

In short, Austria's current eID structure combines two solutions of national ID cards and server-based mobile phone signatures and the mobile phone signature solution is highly used within the country. Mobile phone signature function, which is a server-based e-signature methodology, depends on the basis of two-factor authentication (knowledge & possession) scheme. Signature-creation data (cryptographic keys) are kept at secure HSM devices but controlled by the signatory himself/herself [48] [49]. Although normally server-based method has specific usecase, Rath et al.'s solution's flexibility makes it more applicable in terms of Turkish usecases [15].

CHAPTER 5

5. PROPOSED eID STRUCTURE AND USECASES FOR TURKEY

When we look at the current eID structure in Turkey, we see that different types of solutions are tried to be implemented to different sectors and applications. However, not all of them became widespread as planned. Comparing these present solutions, national ID card solution is the solution that can reach the highest user number so far in Turkey. Citizen cards continue to be distributed in 2019 and total number of citizen ID cards distributed is nearly 37 Million according to the e-population union of public employees [10].

On the other hand, Austria's current eID structure combines two solutions of national ID cards and server-based mobile phone signatures. Mobile phone signature solution is highly used in Austria as it mentioned in the section 4.2. However, citizen card concept also has its advantages when it comes to providing authentication of the citizens in terms of usability and cross-border identification. It is discussed that one of the main advantage of the citizen card is that they are valid across most of the European Union [3]. They provide easy access to another country as well as render unnecessary the passports due to their convenient size [3]. Since, National ID card distributions already have been a part of Turkey's Tenth Development Plan (2014 - 2018) and Turkish e-Government strategy, adopting this joint approach may provide a more realistic and practical solution for Turkey [32].

Therefore, Rath et al.'s server-based eID structure presented in the section 4.2 decided to be used in order to improve the Turkish eID structure and usecases in this part of the study. The modular and flexible concept of Rath et al., and already implemented Austrian server-based eID schemes based on Orthacker et al.'s method allows other countries with different usecase to implement this solution as well [13] [15]. To adopt this solution, first thing to do is identifying the main differences in eID schemes and usecases of Turkey and Austria. A requirements analysis is made in order to specify these differences and propose an alternative eID scheme for Turkey with suitable registration, activation and usage usecases.

5.1. Requirements Analysis for Turkey's EID Structure

Since Rath et al.'s methodology is compatible with the Austrian eID infrastructure, core elements of the Austrian eID environment were determined when evaluating the Turkey's current situation during the analysis. In order to see the difference between Austria's and Turkey's usecases more clearly, the registration, activation and usage scenarios have been examined in detail.

Registration Needs for Turkey

As in other countries, users have to prove their identities with some form of ID's for their legal transactions in Turkey too. Turkish users currently can use their Turkish ID cards (old or new), driving licenses or passports officially. These documents are forms of legal identifications provided in official government domains. On the other hand, Turkish bank accounts also represent a legal identity of users in Turkey and it is a form of identity in private-sector domain. For the registration phase of the solution, Turkish usecase seems to be suitable with the Rath et al.'s method presented in the section 4.2 [15].

- As for the person register service and SIR generation operations, general directorate of population and citizenship affairs is currently responsible for providing legal ID's to Turkish citizens in Turkey. Therefore, this institution can be responsible for handling the registration of the users in this part of the solution. Users can apply to the institution through registration officers face to face as in the first option in the Rath et al.'s solution.
- Self-registration option is provided via smart national identity cards in the proposed solution. Since the beginning of the year 2017, national ID cards for Turkish citizens are started to be distributed. However, there is currently no online environment for Turkish citizens to use in order to create a legal online versions of their IDs or manage them. For instance, if a citizen ID card is lost, owner of the ID needs to go to the general directorate of population and citizenship affairs personally to get a new one. In order to create a new ID for a newborn, people have to apply to general directorate of population and citizenship affairs with a report of birth. As a result, an online registering

application is needed to provide an environment where online eIDs are created and managed.

- Finally, with the third method enabling registration via trusted organizations, it is possible that Turkish citizens' bank accounts can be a source for eIDs. The existing bank accounts of the Turkish citizens can be used to create legal electronic certificates for these citizens. With this method, users having account of any bank can be provided with an online legal eID and electronic signature and there will be no extra effort for these users. Besides Turkish citizens, it is a method also may support the authentication of foreign citizens through trusted organizations worldwide.

Activation Needs for Turkey

Proposed activation process seems applicable for Turkey's usecases. Activation needs to be completed with the help of a certification authority and a person register in the proposed system.

- In Turkey, the national ID database is maintained and ID related operations for Turkish citizens are performed by official General Directorate of Population and Citizenship Affairs Institution. Therefore, creating a central person register is not an issue for Turkey. In the current situation, government already provide a password to the citizens for the use of citizen cards. To make use of the situation, this password can be used to login the person register in the proposed system for Turkey. It is also considered through the study that two-factor authentication can be integrated to the activation process as well. However, this functionality requires phone numbers to be gathered before activation process and also General Directorate of Population and Citizenship Affairs Institution to be integrated with telecom companies in order to handle SMS messages. Therefore, two-factor authentication for the activation process is not considered for the present proposed solution. In addition, the created person register application should also support the legal identities from outside sources such as banks. It should be able to form unique eIDs for each legal person and standardize all kind of eIDs including eIDs from public and private sector.

- The public e-signature keys and certificates of the citizens are currently secured in the databases of six different certification authorities in Turkey. There is no link between the certification authorities' systems and general directorate's system. A central component is needed to establish a connection between official ID records of general directorate and e-signature (public keys, certificates etc.) records of certification authorities.
- E-signature service provided by certification authorities in Turkey is paid. Therefore, proposed solution requires a payment methodology as well. Since current financial operations are handled by CAs themselves, payments can be managed with the help of Central ID Application connecting the payment services of certification authorities in the proposed solution for Turkey. To realize this process, the user should be provided with options of certification authorities in the activation part. Because different users can choose different authorities depending on the service they will use their e-signatures. Then, user is directed to the payment system of the chosen CA by Central ID Application.
- Another difference in the proposed method is the use of HSM. HSM usage is not mandatory according to the Turkish usecases. In the Rath et al.'s case, cryptographic operations are handled in the HSM while six certification authority currently have this responsibility in Turkey. To qualify the proposed method and security standards of it; server-based signature application should integrate HSM into its architecture.
- Another requirement is that the established mobile signature application needs to communicate with three different telecom company in Turkey. In all of the processes in the Rath et al.'s proposed system, phone numbers of the users are used to send OTPs [15]. This activation code is sent to the provided phone numbers of users to establish the base for two-factor authentication.

Usage Needs for Turkey

After registration and activation processes completed, citizens' eIDs are made ready for use. We assume that there is a central ID application and it is connected to the system of the certification authorities and the general directorate of population and citizenship affairs' databases. Besides that, there are multiple eIDs for a single user and each eID has a phone number and unique secret PIN/Passwords linked to it. Following this, some additional requirements are developed for the usage process of the Turkey's proposed solution as a result of this study.

- Currently six certification authority provides software of their own and all of them have different features in Turkey. No common online software can be used to handle electronic signatures. Since central ID application and person register connect the general directorate of population and citizenship affairs' and other public and private institutions in the scheme, it should be developed in collaboration. Proposed structure should provide a common infrastructure where communication between certification authorities, general directorate of population and citizenship affairs' and target applications can be managed securely. In the Austrian method, the component providing these functionalities is MOA-ID [13].
- Rath et al.'s proposed server-based solution includes a web interface to start the e-signing process after receipt of an appropriate HTTP POST [15]. This interface take the phone number and secret PIN/password information from the users and sends a verification code to the users' registered phone number [15]. If the sent code is correctly entered to the interface, electronic signing operations are performed [15]. This kind of interface should be provided within the proposed server-based application.
- The usage process involves the SMS based verification too. Therefore provided server-based application should be able to work with all of the telecom companies (Turkcell, Vodafone, Türk Telekom). Software should support sending SMS messages to the users phone number kept in the person register's database.
- Adopting a new method does not mean that the old method becomes inoperable. Existing electronic signatures of users should be usable in the

context of the new solution as well. Since there is no direct connection between target applications and CA's software anymore, CA's should connect these target applications through the central ID application in the new solution. This transformation is needed to be performed by certification authorities because otherwise each solution would connect the six CA's system separately.

As a result of the requirement analysis performed and side-by-side comparison of the Turkish and Austrian eID schemes, the main necessities of Turkish eID scheme specified as below;

- **A central ID application** in eID structure that provides the integration of Citizen Card Software's systems and general directorate of population and citizenship affairs' system (also connecting the official ID records of general directorate to e-signature data kept on certification authorities).
 - A web interface for central ID application is needed to enable users choose the solution they wanted.
 - It should support both citizen card signatures and server-based signatures.
 - Application should provide a common infrastructure where communication between certification authorities, general directorate of population and citizenship affairs' and target applications can be managed securely.
 - A payment system that is connected to the systems of certification authorities is necessary.
 - It should include a person register component.
 - Person register component should support the registration types; registration via registration officer, self-registration and registration via trusted organization.
 - An online self-registration system for the person register component is necessary to allow users save time and effort. This system also can be used by users for managing their eIDs.
 - Person register application should serve as a common point of contact enabling all outside ID sources 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 HSM device.
 - o HSM usage in the server-based signature solution is needed to improve the security level.
 - o Web interfaces (usage) is necessary to render the server-based signature usage.

5.2. Proposed eID Structure and Usecases for Turkey

Against all differences, modular and flexible solution of Rath et al. ease the implementation of the method and helps us to establish a preliminary eID infrastructure for Turkey [15]. We can draw the proposed eID structure and usecase diagrams for Turkey as in the figures 36, 37 and 38 below;

Proposed EID Structure for Turkey

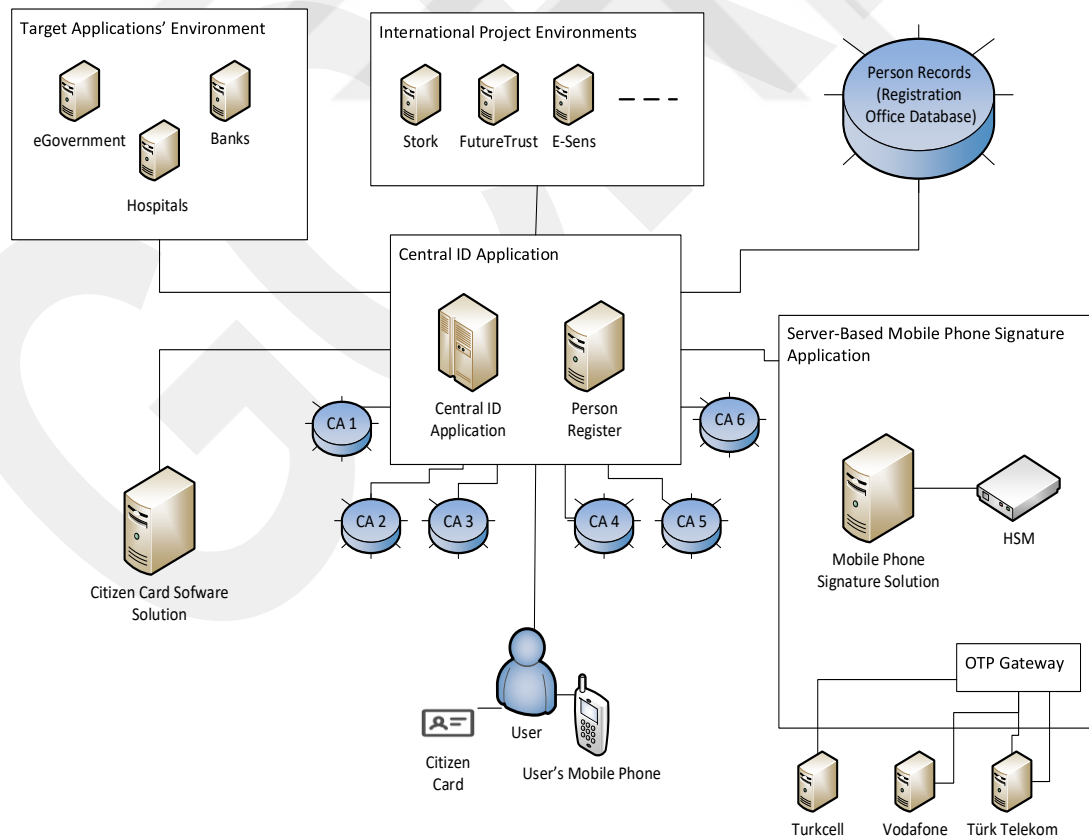


Figure 36 Proposed eID Infrastructure for Turkey

Proposed Usecases for Turkey

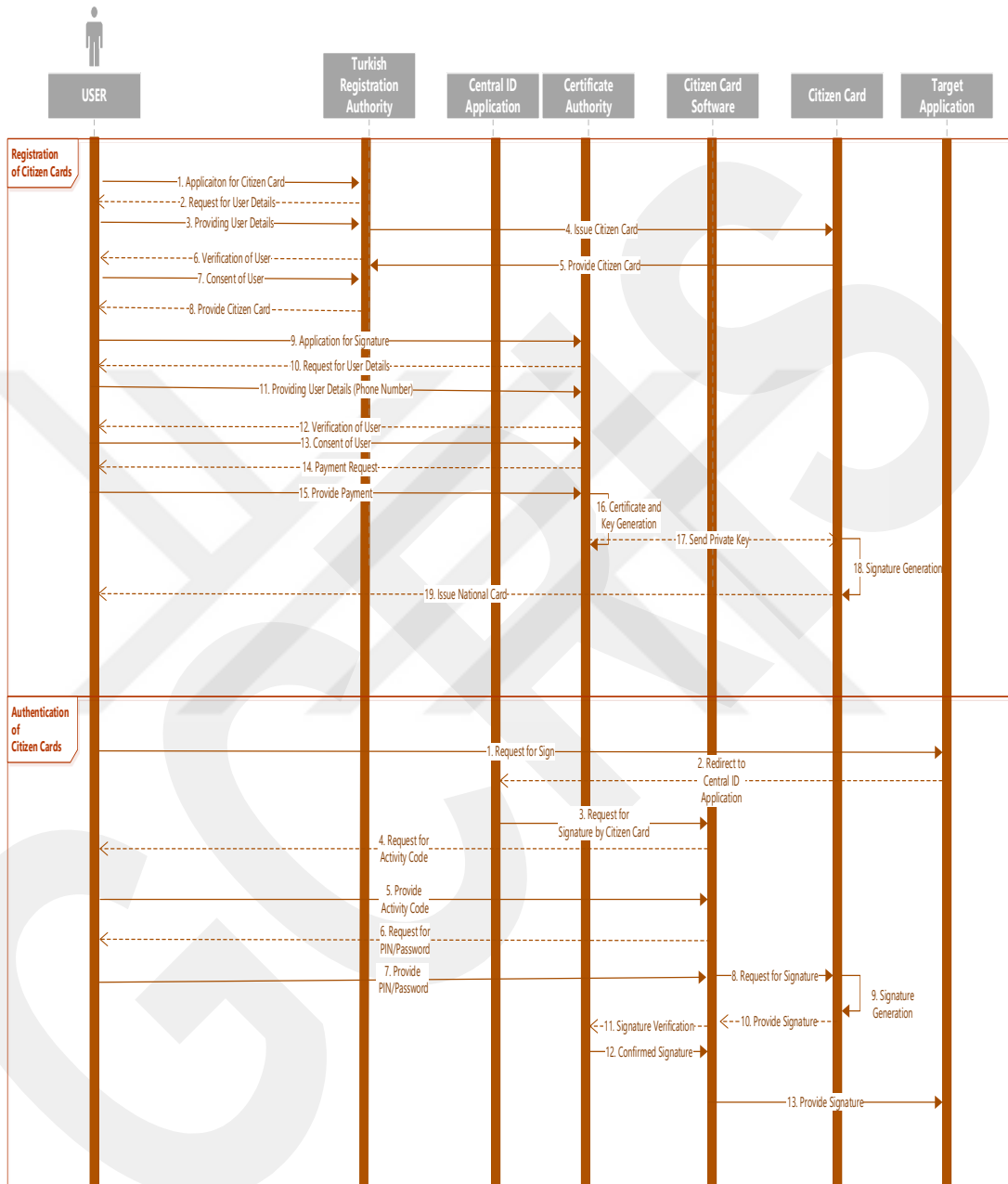


Figure 37 Proposed Registration and Usage Usecases for Citizen Card Signatures for Turkey

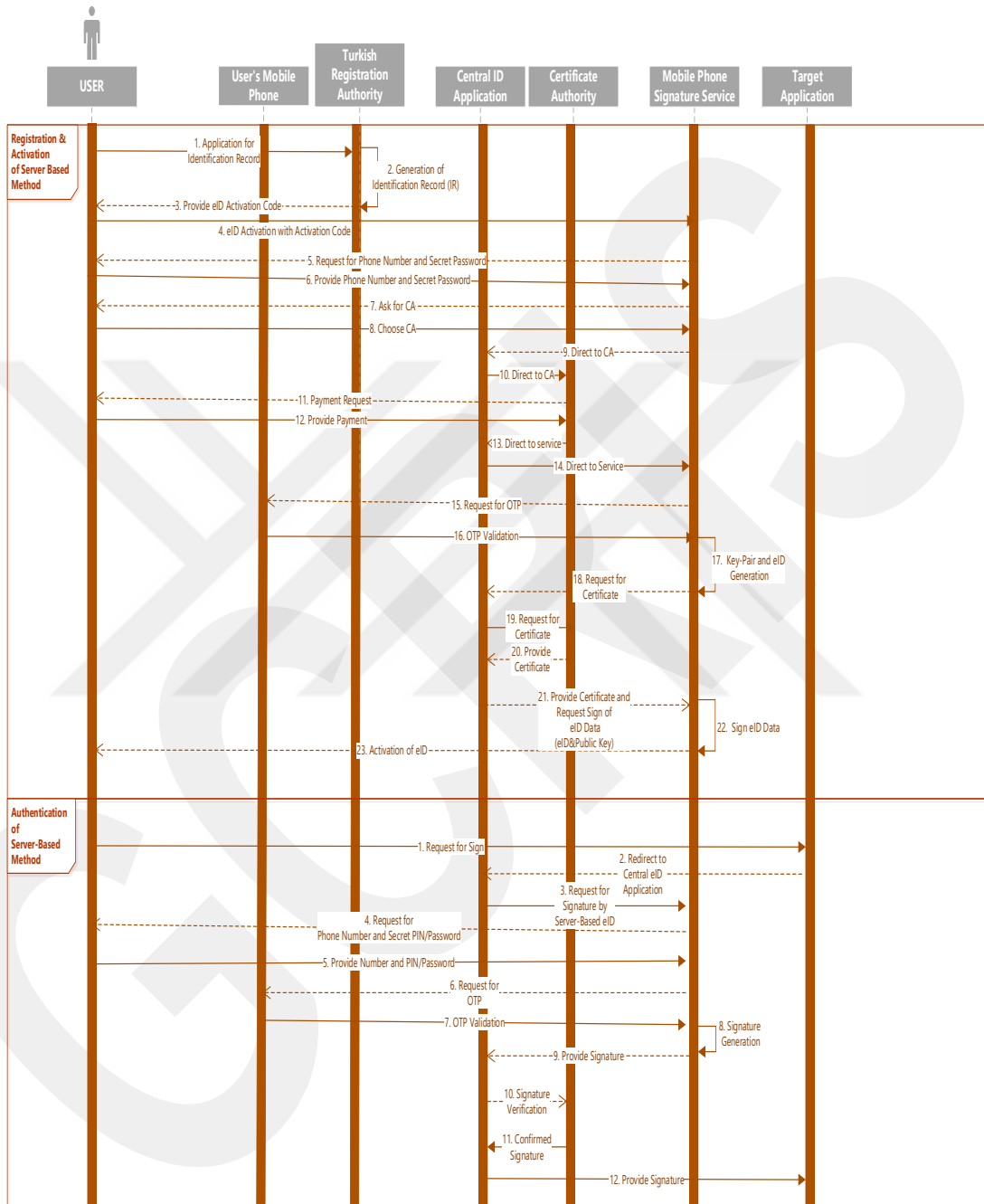


Figure 38 Proposed Registration and Usage Usecases for Server-Based Signatures for Turkey

Registration Phase

In the registration phase, user have two options to identify himself/herself in the solution register step in the proposed solution for Turkey. He/she can use an existing eID or he/she can order a new eID providing his/her legal identification document [19] [15].

Registration Phase – Alternative 1 (Registration via new eID)

1. User goes to a registration authority with his/her identification document such as official IDs, a passport or a driving license.
2. Registration officer conducts face-to-face verification of the user.
3. Officer manually registers the user in the person register system with user's specific data (name, national identification number, phone number etc.) via a web based form.
4. A one-time code is send to the user's provided mobile phone number for validation.
5. If the one time code provided by the user is true, a standard identification record (SIR) and an activation code for the user are created in the person register application.
6. Created SIR and activation code is shared with the server-based mobile phone signature application via SOAP.
7. Activation code is send to the user's mobile phone.
8. Once the user receive the activation code, he/she can login to the proposed server-based mobile phone signature application with his/her phone number and activation code.

Registration Phase – Alternative 2 (Registration via Existing eID)

1. User wants to use his/her existing eID information stored in his/her national ID card.
2. User connect his/her ID card to a card reader and opens person register application provided by central ID application component which is an online environment verifying the user's identity and enabling users to complete the registration on their own.

3. User create a unique account in person register application via a web based form.
4. Identifying information belonging to the user is received from the national ID card and recorded through a web based registration form including name, national identification number, phone number etc.
5. This record is verified through a web service belonging to the person register component in terms of its authenticity because a trusted record should be provided with a signature during registration. User's existing eID is validated through this web service and user's certification authority.
6. If the existing eID is valid, a one-time code is send to the user's provided mobile phone number for validation.
7. If one time code provided by the user is true, a standard identification record (SIR) and an activation code for the user are created in the person register application.
8. Created SIR record and activation code are shared with the server-based mobile phone signature application via SOAP.
9. Activation code is also send to the user's mobile phone.
10. Once the user receive the activation code, he/she can login to the proposed server-based mobile phone signature application with his/her phone number and activation code.

Activation Phase

1. After successful login to the server-based mobile phone signature application, user can start the eID creation process.
2. SIR record is already shared with the mobile phone signature application and there is no eID or signature created up to this point.
3. User fill an activation form in the mobile phone signature application and determine a unique secret password together with a revocation password to create an eID for himself/herself.
4. If the user already have an existing eID (Registration alternative 2), he/she does not need to choose a certification authority.
5. If the user does not have an existing eID (Registration alternative 1), he/she choose a certification authority in the activation form.

6. User is directed to the chosen certification authority's payment system to complete the necessary payments.
7. After the activation form is completed in the mobile phone signature application, a one-time code is send to the user's provided mobile phone number for validation.
8. If the one time code provided by the user is true, a signing key-pair generated in the HSM ((Priv_{Sig}) and (Pub_{Sig})) and an encryption key pair ($K(\text{Priv}_{User})$ and $K(\text{Pub}_{User})$) for the user is created in the application server.
9. A certificate for that user's eID is also created by the help of certification authority.
10. After an eID is created for the user, it contains specific phone number and secret and revocation passwords information besides the personal information of that user transferred from person register.
11. At the end of the process, created eID and keys are encrypted.
12. All encrypted entities is stored under the server-based application securely.

Activation Phase – Encryption

Notations:

$User(\text{Priv}_{Sig})$ and $User(\text{Pub}_{Sig})$: Signing key pair created in the HSM

$User(\text{Priv}_{Enc})$ and $User(\text{Pub}_{Enc})$: Encryption key pair created in the application server

SP: Secret password chosen by the user

$CA(\text{Priv}_{Sig})$ and $CA(\text{Pub}_{Sig})$: Key pair given by the certification authority within the system

R: A random generated number used against replay attacks

HSM_{MK} : Master key of the HSM

$E\{a,b\}$ is used for asymmetric encryption; a represents the encrypted data while b represents the key $D\{a,b\}$ for asymmetric decryption

$E(a,b)$ is used for symmetric encryption such as AES

Encryption: The user private signing key is stored in the HSM Module (encrypted with HSM's master key)

$$E\{ User^{(Priv)}_{Sig}, HSM_{MK} \} = Q$$

$$E\{ Q, User^{(Pub)}_{Enc} \} = T$$

A signature certificate is requested from the chosen (or existing) CA and certificate is stored in Central Application

$$E\{ (User^{(Pub)}_{Sig} + eID \text{ data}), CA^{(Priv)}_{Sig} \} = S$$

User's private key is encrypted using symmetric encryption with hash of user's secret password

$$E(User^{(Priv)}_{Enc}, \text{hash}(SP)) = G$$

Using generated random number, R, S is encrypted

$$E(S, R) = H$$

R is also encrypted using User public encryption key

$$E\{ R, User^{(Pub)}_{Enc} \} = K$$

After the completion of the operations showed is above steps; T, G, H, K and a certificate are stored within the system.

Authentication (Signing) Phase

1. If a user wants to perform an electronic signature through server-based method, first he/she should complete the activation process and create a unique eID for himself/herself.
2. If a user wants to sign a document or prove his/her identity in a platform, user opens the central ID application page. (or the web interface of central ID application can be implemented in target applications)
3. Firstly, user choose and upload the document that he/she wants to sign.

4. After uploading the document, user is asked whether he/she wants to sign with server-based or national card based authentication option via the interface provided by central ID application.
5. If server-based authentication method is chosen, the signature-creation starts with an HTTP request to the web interface provided by the server-based mobile phone signature application.
6. In the web interface of mobile phone signature application, user is asked to provide his/her phone number and the secret password.
7. Phone number and secret password data send to the server-based signature application server via HTTP connection.
8. If the given information is corresponds to an eID record in the system, user receive an OTP to his/her mobile phone.
9. After that, user is required to provide correct one-time password (OTP) in the web interface. During these process, a unique reference value is also created and this value is showed to the user in both web interface and in SMS message. This reference value is used to prevent man-in-the-middle attacks.
10. Then, he/she should provide the one time password to the solution to complete the signing process and perform a two-factor authentication.
11. If all of the provided information is verified within the system, electronic signature is performed on behalf of the user inside the HSM module and signed data is transferred to the target application through central ID application.
12. The authentication processes is given below in detail.

Authentication (Signing) Phase – Decryption

After the completion of the activation phase; B, G, H, K and a certificate were already stored within the system.

1. $D (G, \text{hash}(\text{SP})) = User_{Enc}^{(Priv)}$
2. $D \{ K, User_{Enc}^{(Priv)} \} = R$
3. $D (H, R) = S$
4. $D \{ S, CA_{sig}^{(Pub)} \} = User_{sig}^{(Pub)} + eID \text{ data}$

$$5. D \{ T, User_{Enc}^{(Priv)} \} = Q$$

$$6. D \{ Q, HSM_{MK} \} = User_{Sig}^{(Priv)}$$

Usecase for Revocation

Method itself includes case of revocation. In the proposed method, a revocation password is determined by the end user during the activation phase together with the secret password. This way, in the event of losing or forgetting the actual secret password, user can demand to change his/her password through this revocation password. User needs to provide his/her phone number with the previously determined revocation password into the proposed method first. After that user is authenticated via one time password through provided phone number. If the provided code from user is true then, user is directed to the password renewal interface. If the revocation password is forgotten or lost too, then the person is needed to pay a visit to the registration authority in person with an identification document to authenticate face to face. The new password is provided to user after authentication.

Usecase for Disabled Users

Disabilities are important sides of the study since identification and authentication should be provided for everyone. In Turkey disable people are provided with their identification document but sometimes they may not have in position to perform legal processes due to their limitations. In that case they have legal guardian according to their disability. Today in Turkey, disabled people can not be provided with e-signatures legally. Instead of that, their legal guardians perform their necessary operations on behalf of them. In the proposed solution the activation of an eID is only possible if the user is not specified as disabled. Disabled people can still register the application, create a unique record for themselves and provide their unique ID information however they can not apply e-signatures. If a signature is needed for application, their legal guardian's signature is necessary.

Usecase for Underage Users

Today in Turkey, underage people (age of eighteen) have their identification documents for themselves however they can not be provided with e-signatures legally. Because of that providing an eID for underage is problematic because if an underage person applies electronic signatures online, it will not be legal. In the proposed solution the activation of an eID is only possible if the user is above eighteen years old. Under age can still register the application, create a unique record for

themselves and provide their unique ID information however they can not apply e-signatures. If a signature is needed for application, their parents or legal guardian's signature is necessary. Every Turkish citizen reached legal age, every citizens or foreigners, can get their activation code from the authorized branches if they apply to the Population Directorate in person later.

Usecase for Foreign Users

Today, because of Turkey is not a European Union country, the cross-border identification of foreign citizens are made face to face only, through passports. In the Turkey's identification structure; adopting a centralized and server-based method would bring some advantages to the Turkey's current eID scheme increasing the cross-border interoperability. The proposed system provides an alternative option where identification attributes can be read directly from the foreign ID card with a qualified certificate [13] [15]. If a foreigner wants to authenticate in Turkey via proposed method, he/she could use him/her existing national ID card to register the proposed system and create a unique eID for himself/herself.

In the registration phase, can use an existing eID. Firstly identifying information belonging to the foreign user is taken through a web based registration form [19] [15]. The user specifies whether he/she is a foreign user in the registration form. The component responsible for the registration of the users and standardizing the records from different resources is called person register system [19] [15]. After user provided his/her personal information and a binding phone number, a unique identification record is constituted in the person register system [19] [15]. This record is verified through a web service belonging to the person register component in terms of its authenticity because a trusted record should be provided from a trusted organization with a signature [19] [15]. In that particular case, the foreign user's identity information is verified through International project environments as it shown in the figure 36. An activation code is given to user to enable his/her login to the activation system later [19] [15].

After registration of the user is completed and a valid identification record is stored in the person register component and it is marked as the foreign user. User can login to the activation system, which is a web based interface, with his/her phone number and activation code [19] [15]. During the activation, user needs to choose a secret password and a revocation password to create an eID for himself/herself [19] [15].

After a secret password is chosen by the user, an SMS authentication is performed within the activation system [19] [15]. An OTP (One Time Password) is send to the person's registered mobile phone and it is verified since it will be used in the authentication process later [19] [15]. If the SMS authentication is completed without an error, the key-pair creation and signature application is applied as mentioned before

5.3. Applicability of the Proposed Method

In the previous section, an alternative identity authentication scheme for Turkey is presented. The use of a hybrid solution of national ID cards and server-based mobile e-signatures is proposed. As a part of this study, the applicability of the proposed structure in Turkey is investigated. In this case, applicability means that the compatibleness of the usecases to Turkey's legal, technical and security grounds.

5.3.1. Legal Framework

In order to increase the use of e-signatures and to standardize e-signature processes in Turkey, legal regulations are prepared and controlled as well as projects are conducted for the implementation of these legislations. For example; EU Directive 1999/93 / EC, which is the basis of the legal and technical framework of the electronic signatures, are accepted and the law corresponding to this directive and its articles is defined in Turkish national legislation [23]. The 2016-2019 National e-Government Strategy and Action Plan is put in use with the help of Scientific and Technological Research Council of Turkey (TUBİTAK-UEKAE) to investigate the new technological developments and global trends [32] under the light of this directive. The Information Society Strategy and Action Plan was also approved and this program aimed to achieve efficiency and user centricity when delivering e-Services in Turkey [32]. E-Government structure of Turkey is also covered in the Turkey's Tenth Development Plan for the years 2014 to 2018 [32]. Besides this legal studies, several projects are carried out such as e-government project, national citizen card projects etc. to meet the requirements arising from this directive.

As a result of these efforts, Turkey's legal structure seems ready to implement proposed eID structure. However, there are still inadequacies on some issues needed to be improved in the legal e-signature framework of the Turkey.

- With the eIDAS Regulation which was accepted in the European Parliament on 23/07/2014 and entered into force on 1/07/2016 [6]; in addition to issues relating to the mutual recognition of electronic identities in EU member states, other aspects of trust services such as time stamps, registered electronic delivery services, different authentication structures also have been regulated [23]. As of the date of its entry into force, the eIDAS Regulation revokes the EU Directive 1999/93/EC, which is the basis of the legal and technical framework of electronic signatures in Turkey [23]. In this context, the "Report on the Regulation of Trust Services" was prepared by the Information Technologies Department in 2018 [23]. Within the scope of harmonization of the Turkey's laws with EU legislation; updates on trust services in Turkey's laws in line with eIDAS must be completed.
- The fact that Austria's' technical infrastructure (server-based e-signatures using HSM) is now considered a reliable and valid system according to eIDAS, supports the applicability of the proposed solution for Turkey. Since there is already a need for a structure compatible with eIDAS, proposed structure is a good solution to handle the legal and technical obstacles.
- The proposed server-based eID infrastructure is a product of public-private partnership in Austria [48]. In order to combine public and private sectors and create a homogeneous structure throughout the country, public-private partnership projects should be initiated and these projects should be managed and audited by the government. As it is mentioned in the study of Polanski, Unification of e-trust services requires adoption and cooperation between states and private parties rather than difficult implementations [22]. Governmental management of such projects is important because; although legal framework is constituted in a timely manner, use of e-signature may not reach the expected levels due to insecurity in new technologies [9].

5.3.2. Technical Framework

Requirements of the Austria's' method and presented server-based method for Turkey are similar in terms of technicality. However, the following factors should be considered to evaluate method's availability in Turkey.

- Since 2017, Turkey have distributed about 37 Million Citizen cards with e-signature functionality to its citizens [10]. Proposed solution combines the citizen card concept and the server-based mobile phone signature concept. Since there is no need for changing the current infrastructure, implementation of this method should be easier.
- Proposed solution is based on Austria's server-based authentication methodology, which has been implemented and used for many years. Austria's e-signature usecase, which has been working reliably since 2009, is one of the factors supporting the applicability of the proposed e-signing structure [15]. Besides that, many studies are have been completed to evaluate and approve the usability and security level of Austria's system since then [16] [21] [13]. The usability analysis are given by Zefferer in the year 2012 [16] while Stipsits make a detailed security analysis of the Austria's citizen card solution in the year 2015 [21]. Therefore proof of concept is already achieved for this structure.
- The general technical components used in the Austria's eID environment and the choice of technologies are specifically chosen from international and well known standards such as *SOAP/WSDL Web services, SSL, SAML3 or electronic signature standards such as XMLDSIG4 or XAdES5* [13]. The advantages of this approach mentioned in the study of Stranacher et al. as *"Austria tries to guarantee technology neutrality in its e-Government solutions. This neutrality is guaranteed by open interfaces and easy exchangeability of single modules."* and *"On the one hand, such standards ensure interoperability between cross-domain applications of public authorities. On the other hand, well-established and proven standards ascertain a high level of security and privacy for citizens."* [13].

- Difference between population sizes of Austria and Turkey is a limitation of the proposed method. The national population size of Austria is nearly 8,82 million in 2018 when Turkey's population is nearly 80,81 million in 2018. Handling the identities of ten time bigger population is harder in terms of technical structure of the solution. While population size shows itself as a drawback of the proposed method, more advanced and additional distributed systems can be considered to offer a solution to this problem.
- Based on the information provided in this section, eID and personal information management issue should be handled in a standardized and safe way to ease cross-border applicability. Combination of new technologies like Internet of Things (IoT) applications and block-chain mechanisms are suggested to utilize this kind of information sharing processes in Medeni et al.'s study [28]. To reach a smarter and more secure cross-country eID system, these technologies could be considered.

5.3.3. Security Framework

Presented server-based identity authentication scheme for Turkey based on the grounds of Austrian citizen card concept together with Orthacker et al.'s Qualified Mobile Server Signature concept [19]. Server-based concept, which is presented in section five, simply relies on HSM modules instead of SIM cards or smart cards to secure the cryptographic operations [19]. Possession factor is met by HSM and OTP (One-time password) sent via SMS together, while knowledge factor is met by users' secret PIN/Password. Since the infrastructure of the solution proposed for Turkey is based on the methods and infrastructure of Austrian eID concept, security analysis and its results performed by Orthacker et al.'s, Rath et al., and Stipsits are substantial for this thesis [19] [50] [15] [21].

- In Orthacker et al.'s study, they discussed the security measures of the proposed system and stated that security of the SMS function constitutes probably the weakest link due to existence of GSM encryption attacks [19]. In 2014, Rath et al. presented a flexible and modular alternative to Orthacker et al.'s method but the main disadvantage of the system still presented as SMS-based user-authentication in terms of security due to its vulnerability against malware [15]. In this regard, Rath et al. recently presented another study to

improve the security of the system [50]. They discussed encryption-based authentication instead of SMS based authentication in their study [50]. Therefore, the proposed solution for Turkey can be further improved in this manner.

- As for the security of the citizen card method in the concept; Thomas Johannes Stipsits from the Faculty of Informatics at the Vienna University of Technology perform another detailed security analysis of the Austrian eID system [21]. In the thesis named “Security Analysis of the Austrian Citizen Card Environment MOCCA and E-Card”, Potential leaks of MOCCA (Modular Open Citizen Card Architecture) software were discussed, and its vulnerability was evaluated [21]. According to the study’s results, fake applet attacks considered as the main weakness of the citizen card system [21].

Improved Security for Turkey

According to the 2018 Digital Government Factsheets report prepared by European commission, the percentage of households with internet access in Turkey for 2017 is near 80% which is very close to the rate of EU [31]. Besides households; according to the given numbers, people who work in these enterprises use the internet for banking and financing services with the percentages %77,5, %77.6, %76.3, %78.1 respect to the years 2007, 2008, 2009, 2010 [31]. According to the Clare Sullivan, digital identity concept is supported not only cost and efficiency purposes but also to reduce fraud [51]. Regardless of which identity validation approach is used, same digital identities used for government services will also be used for transactions made in the private sector [51]. As a result of these numbers, the security measures gained importance for ensuring the integrity of the user’s privacy of identity in Turkey.

- There are different e-signature solutions applied by different institutions such as banks, trading sites (shares, stocks), ticket sales (hotels, airplanes), shopping sites, health sector and government institutions in Turkey. For instance, shopping sites use only single secret passwords to authenticate their customer while electronic prescriptions are used via smartcard-based e-signatures in the hospitals. This situation causes different security levels for

different applications. The centralized eID architecture of the Austrian eID scheme provides a common environment where all applications (private or public) can benefit from. Therefore, the proposed system for Turkey also offers a solution to the different security levels.

- In Zefferer's study on Austria's eID scheme, the security level of the Austrian eID system is also evaluated [16]. Users who have been asked to use the three different implementations (MOCCA Local, MOCCA Online and Mobile Phone Signature), have rated the perceived level of security and trustworthiness [16]. According to the results of the study, mobile phone signature implementation (which is a server-based e-signature creation) considered the most secure implementation by test users as it shown in the figure 39 [16]. In conclusion, the Austrian server-based eID method is considered as a secure way of identification in the eyes of people as well as according to its analysis performed and experience of Austria.



Figure 39 Security Evaluation Results of MOCCA [16]

5.4. Contribution to the Current EID Structure of Turkey

According to the FORMIT foundation's study report prepared by European Commission in 2013, in the matter of e-signature products, there are three factors that need to be taken into account and harmonized in order to find the optimal point of balance [1]. These factors are "usability", "security" and "interoperability" [1]. Main

contributions of the proposed system for Turkey's electronic signature scheme are **usability increase** and **cross-border interoperability** besides a sufficient level of security increase accordingly.

According to the 2019 Digital Government Factsheets report prepared by European commission, a comparison was made between the development of e-Government in Turkey and in EU [52]. As it seems, indicator of User Centricity is scored 85 for Turkey, while it is 82 for EU countries' average [52]. In addition, Citizen Cross-Border Mobility indicator score is 35, while EU countries' average score is 48 [52].



Figure 40 e-Government Benchmark Report 2018 Country Factsheet for Turkey [52]

On the other side in Austria's case, these user centricity and citizen cross-border mobility indicators are met by 92 for user centricity and 69 for citizen cross-border mobility indicator. Therefore, we can say that there is still a gap in terms of usability and cross-border interoperability between Turkey and EU countries [32].



Figure 41 e-Government Benchmark Report 2018 Country Factsheet for Austria [52]

Contribution to Usability

As for the contribution to the usability factor; adopting Austria's centralized and server-based method would bring some advantages to the Turkey's current eID scheme.

- People had to create accounts for each online services, which results in numerous online identities over the internet. With the help of centralized e-identity management technologies enabling single eID for multiple services, people freed from the burden of creating different accounts and managing multiple passwords for services.
- Existing separate identification structures and the lack of standards causes fragmentation in Turkey [3]. This results in data repetition all over institutions such as hospitals, telecom companies, banks etc. and inconsistencies. To solve this issue, Central ID Application component proposed in the section 5.2 of this study, provides a central management of online identities by connecting different parties and standardizing the processes. Since proposed server-based methodology offers central management of eID services with proper standards, the integration of these separate services is provided at a sufficient

level. As a result, people do not have to provide information about themselves in different institutions repeatedly so usability is improved.

- In addition, proposed server-based method provides a flexible environment in terms of hardware usage. Even if National ID cards are liable solution as it is capable of creating electronic signatures as well as being valid in most of the European Union countries, it requires card-reading machines to work [20] [10]. Smart card reader's problems (software, distribution etc.) occupied Estonia for a long time [53]. Server-based e-signature approach provides an alternative to citizen cards to eliminate these kind of problems. Since no reader or additional software are required of users, server-based signature is a comparatively cheap, user-friendly, and a flexible solution.
- Since server-based methodology uses SMS messages in its authentication process, smart phones are not required on the contrary of SIM card based mobile signature methods. This solution can be implemented with non-smart phones as well. This convenience improves usability by extending the sphere of influence.
- Since proposed server-based e-signature method is already implemented in Austria, there have been studies evaluating the usability of the implementations. The usability level of the Austrian eID system is evaluated in Zefferer's study on Austria's eID scheme [16]. There were three different implementations (MOCCA Local, MOCCA Online and Mobile Phone Signature) of Austrian e-government application and the usability scores given by users were as it shown in the figure 42 [16]. Consequently, mobile phone signature (which is a server-based e-signature creation) rated as the most

usable implementation in most categories (intuitive, trustworthy, positive, clear, not frustrating, familiar, and fast) by test participants [16].

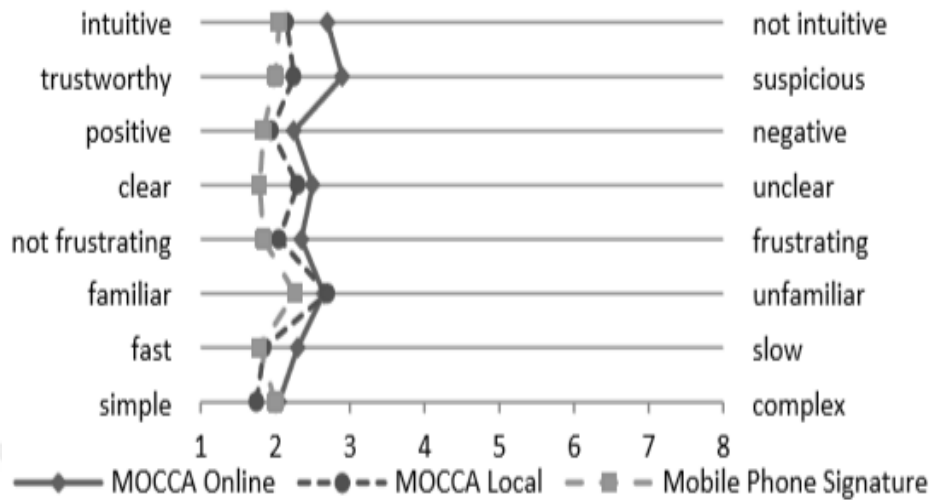


Figure 42 Perceived Usability of Different Implementations of Austrian e-Government [16]

Contribution to Cross-Border Functionality

Besides usability problems, Turkish eID structure needs to be improved in terms of cross-border interoperability. The main problem may cause that incapability is explained in the Leitold's study as *"The national eID infrastructure often emerged in isolation, developed only to meet sectorial, regional, or national requirements. Using the eID tokens – whatever the technological implementation is (card, mobile phone, etc.)– across borders was no priority for most states."* [24]. In the Turkey's case; different e-signature implementations of smart cards, mobile methods (SIM cards), national ID cards and oAuth methods make the general process more complex and it is getting harder to reach an international and easy way of online identification for Turkey.

As for the contribution to the cross-border interoperability; adopting a centralized and server-based method would bring some advantages to the Turkey's current eID scheme.

- Because of Turkey is not a European Union country, the cross-border identification of foreign citizens are made face to face only, through passports. Since the proposed eID structure for Turkey base upon national citizen cards

and server-based mobile signatures concepts together, it makes online identification easier for foreign citizens. For registration of the foreign users, the adopted system provides an alternative option where identification attributes can be read directly from the foreign ID card with a qualified certificate [13] [15]. Thanks to this self-registration functionality, personal presence of foreign users is not required in public administrations [13] [15].

- The Central ID Application component in the eID scheme, which is a central service combining e-signature authorities and citizen register authorities; allows citizens to connect government or private corporation applications through single path. People do not need to register different applications. Central ID management stores the necessary identification data (ID number, name, phone etc.) and provides the legal data of that person to needed application when the person authorizes it. This solution prevents different levels of information in different systems in national level as much as it supports the collection of homogeneous data for the Member States in European level.
- With the introduction of eIDAS regulation replacing the old eSignature Directive (1999/93/EC) across Europe, national electronic identification schemes are considered valid in other EU countries where qualified e-signatures are available [6]. Adopting the Austrian server-based eID methodology fits the eIDAS regulation, increases the cross-border operability of the system as well as provides legal structure for Turkey. Today, laws of Turkey includes only electronic signatures depending upon the Directive 1999/93/EC [2] [8]. However, with the enforcement of eIDAS regulation, all types of e-signatures and international eID schemes would be described and supported [6].

As a result, besides other advantages of server-based eID methodology, a cross-border and eIDAS compliant infrastructure is possible with proposed eID system.

CHAPTER 6

6. CONCLUSION

Besides the inadequacy of Turkish eID structure when recognizing international identities, Turkey also has lagged behind in other countries in terms of usability. It is seen that, in the current eID structure of Turkey, different types of electronic signature solutions are tried to be implemented to different sectors and applications but not all of them became widespread as planned. To deal with these problems, an Austrian server-based eID approach which is a combination of national ID cards and mobile signatures, is investigated in terms of its possible contributions to Turkey's current eID scheme. Main necessities of current Turkish eID scheme identified to improve the eID infrastructure towards Austrian case. Considering the current structure and necessities, a new eID infrastructure and usecase scenarios consistent with the existing structure of Turkey, are designed.

A server-based eID structure for Turkey is presented with the help of Austrian server-based eID approach, Orthacker et al.'s qualified mobile server signature concept [19] [15] and Rath et al.'s flexible concept for mobile eID and e-signature solutions [15]. It is observed that, the designed eID structure for Turkey, providing the same functions of the Austrian eID scheme, could be achieved with some modifications of the current Turkish eID structure and it is concluded that the proposed eID structure for Turkey is applicable with its legal and technical frameworks. According to the requirement analysis conducted in the research; a central ID application in eID structure that provides the integration of Citizen Card Software's systems and general directorate of population and citizenship affairs' system and a server-based signature application that is capable of creating server-based e-signatures in HSM device are concluded as the main necessities.

The proposed system based on Austria's eID offers effective solutions to problems in the areas of usability and cross-border interoperability. With the help of centralized e-identity management technologies enabling single eID for multiple services, people freed from the burden of managing too many passwords and they do not have to

provide personal information in different institutions repeatedly. In addition, no reader, no smart phone or additional software and hardware are required of users in the server-based solution, server-based signatures are a comparatively cheap, user-friendly, and a flexible solution. Besides the usability contributions, presented system provides an alternative option where identification attributes can be read directly from the foreign ID card with a qualified certificate [13] [15]. Thanks to this functionality cross-border signatures are supported by the server-based method. Central ID management stores the necessary identification data of people and provides the necessary data of that person to needed application when the person authorizes it. By this function, this solution also prevents different levels of information in different systems in national level as much as it supports the collection of homogeneous data for the Member States in European level. Additionally, with the introduction of eIDAS regulation replacing the old eSignature Directive (1999/93/EC) across Europe, proposed server-based eID methodology fits the eIDAS regulation, increases the cross-border operability of the system as well as provides legal structure for Turkey.

In conclusion, to achieve such system, government and private sector actors should work together, the integration between the central register authority of Turkey and six certification authority should be constituted and legal legislation should be brought in line with international standards as soon as possible. One technical limitation discussed during the study is the difference between population sizes of Austria and Turkey. It is concluded that more advanced and additional distributed systems can be considered to offer a solution to this problem.

REFERENCES

- [1] FORMIT Foundation, "eSignature Study on the supply side of EU e-signature market - Final Study Report" European Commission Directorate-General Information Society and Media, Rome, 2013.
- [2] European Union, "Directive 1999/93/EC of the European Parliament and of the Council" 8 August 2019. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31999L0093>.
- [3] The World Bank Group, "Estonia A Successfully Integrated Population-Registration And Identity Management System Delivering Public Services Effectively" The World Bank Group, Washington, 2015.
- [4] seesign, "two-factor-authentication" 8 August 2019. [Online]. Available: <https://www.secsign.com/business/two-factor-authentication/>.
- [5] CEF Digital, "CEF Digital" 8 August 2019. [Online]. Available: <https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Large+Scale+Pilot>.
- [6] European Union, "eid.as" 8 August 2019. [Online]. Available: <https://www.eid.as/home/>.
- [7] D. Hühnlein, T. Frosch, J. Schwenk, C.-M. Piswanger, M. Sel, T. Hühnlein, T. Wich, D. Nemmert, R. Lottes, S. Baszanowski, V. Zeuner, M. Rauh, J. Somorovsky, V. Mladenov and C. Condovici, "FutureTrust–FutureTrust Services for Trustworthy Global Transactions" in *Open Identity Summit 2016*, Bonn, 2016.
- [8] BTK, "BTK" 8 August 2019. [Online]. Available: <https://www.btk.gov.tr/>.
- [9] D. Kabasakal, "Elektronik İmzadan Mobil Elektronik İmzaya Geçiş Sürecindeki Yansımalar, Uygulamalar ve Öneriler" Bilgi Teknolojileri ve İletişim Kurumu, Ankara, 2007.
- [10] TC İçişleri Bakanlığı - Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü, "TC İçişleri Bakanlığı - Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü" 2019 August 2019. [Online]. Available: <https://www.nvi.gov.tr/>.
- [11] BTK, "BTK/elektronik-sertifika-hizmet-saglayicilari" 8 August 2019. [Online]. Available: <https://www.btk.gov.tr/elektronik-sertifika-hizmet-saglayicilari>.

- [12] IBM Knowledge Center, "Identification and authentication" 8 August 2019. [Online]. Available: https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009740_.htm.
- [13] K. Stranacher, T. Zefferer, A. Tauber and B. Zwattendorfer, "The Austrian Identity Ecosystem: An E-Government Experience" *Architectures and Protocols for Secure Information Technology Infrastructures*, pp. 289-309, 2013.
- [14] Ş. Sağıroğlu, D. Kabasakal and M. Alkan, "Mobil Elektronik İmza, Altyapısı ve Türkiye" *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, pp. 49-56, 2008.
- [15] C. Rath, S. Roth, M. Schallar and T. Zefferer, "Design and Application of a Secure and Flexible Server-Based Mobile eID and e-Signature Solution" *International Journal on Advances in Security*, pp. 50-61, 2014.
- [16] T. Zefferer and V. Krnjic, "Usability Evaluation Of Electronic Signature Based E-Government Solutions" in *IADIS International Conference*, Madrid, 2012.
- [17] A. Ruiz-Martínez, D. Sánchez-Martínez, M. Martínez-Montesinos and A. F. Gómez-Skarmeta, "A Survey of Electronic Signature Solutions in Mobile Devices" *Journal of Theoretical and Applied Electronic Commerce Research*, pp. 94-109, 2007.
- [18] P. Teufl, T. Zefferer, C. Woergoetter, A. Oprisnik and D. Hein, "Android - On-device detection of SMS catchers and sniffers" in *International Conference on Privacy & Security in Mobile Systems*, Aalborg, Denmark, 2014.
- [19] C. Orthacker, M. Centner and C. Kittl, "Qualified Mobile Server Signature" in *25th IFIP TC 11 International Information Security Conference (SEC)*, Brisbane, 2010.
- [20] H. Roßnagel, J. Camenisch, L. Fritsch, T. Gross, D. Houdeau, D. Hühnlein, A. Lehmann and J. Shamah, "FutureID – Shaping the Future of Electronic Identity" 2011.
- [21] T. Johannes Stipsits and M. Kammerstetter, "Security Analysis of the Austrian Citizen Card Environment MOCCA and E-Card," Technische Universität Wien, Wien, 2015.
- [22] P. Polanski, "Towards the single digital market for e-identification and trust services" *Computer Law & Security Review*, vol. 31, pp. 773-781, 2015.
- [23] Bilgi Teknolojileri ve İletişim Kurumu, "Bilgi Teknolojileri ve İletişim Kurumu 2018 Faaliyet Raporu" Bilgi Teknolojileri ve İletişim Kurumu, Ankara, 2018.
- [24] H. Leitold, "Challenges of eID Interoperability: The STORK Project" Graz, 2011.

- [25] A. Rodríguez and Miguel, "STORK - Secure Identity Across Borders Linked" *OECD Seminar on eID*, Paris, 2008.
- [26] European Union, "STORK | Take your e-identity with you, everywhere in the EU" 8 August 2019. [Online]. Available: <https://ec.europa.eu/digital-single-market/en/content/stork-take-your-e-identity-you-everywhere-eu>.
- [27] European Union, "esens.eu" 8 August 2019. [Online]. Available: <https://www.esens.eu/content/first-cross-border-eidas-compliant-connections-achieved>.
- [28] T. Medeni, T. Medeni and D. Soylu, "Reflections And Suggestions On Cross-Country Electronic Services For Transportation, Logistics And Food Supply Chain" *Journal of Naval Sciences and Engineering*, vol. 14, no. 2, pp. 100-109, 2018.
- [29] EEMA - the European Association for e-Identity & Security, "FutureTrust Project" 8 August 2019. [Online]. Available: <https://www.futuretrust.eu/>.
- [30] European Union, "Digital Government Factsheets" 8 August 2019. [Online]. Available: <https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/digital-government-factsheets-2018>.
- [31] [bilgitoplumu.gov.tr](http://www.bilgitoplumu.gov.tr), "bilgitoplumu.gov.tr" 8 August 2019. [Online]. Available: http://www.bilgitoplumu.gov.tr/wp-content/uploads/2014/04/Bilgi_Toplumu_Istatistikleri_2011.pdf.
- [32] European Commission, "eGovernment in Turkey" European Commission, 2019.
- [33] A-SIT Secure Information Technology Center - Austria, "Mobile Phone Signature & Citizen Card" 8 August 2019. [Online]. Available: <https://www.buergerkarte.at/en/index.html>.
- [34] E. eID, "Estonia eID" 8 August 2019. [Online]. Available: <http://www.id.ee/?lang=en>.
- [35] Belgium eID, "beID" 8 August 2019. [Online]. Available: <https://eid.belgium.be/en>.
- [36] Spanish eID, "National Police Body" 8 August 2019. [Online]. Available: <https://www.dnielectronico.es/PortalDNIE/>.
- [37] M. Mutlugün and O. Adalier, "Turkish National Electronic Identity Card" in *2nd International Conference on Security of Information and Networks*, Gazimagusa, 2009.
- [38] T. E-Government, "Turkish E-Government" 8 August 2019. [Online]. Available: <https://www.turkiye.gov.tr/>.
- [39] Bilgi Teknolojileri ve İletişim Kurumu, "Türkiye Elektronik Haberleşme Sektörü - Üç Aylık Pazar Verileri Raporu" Bilgi Teknolojileri ve İletişim Kurumu, 2019.

- [40] e-tugra, "helpdesk e-tugra" 8 August 2019. [Online]. Available: .. <https://helpdesk.e-tugra.com.tr/>.
- [41] kamusm, "yazilim kamusm" 8 August 2019. [Online]. Available: <https://yazilim.kamusm.gov.tr/>.
- [42] turktrust, "turktrust" 8 August 2019. [Online]. Available: <https://www.turktrust.com.tr/tr/>.
- [43] S. Arora, "National e-ID card schemes: A European overview" Elsevier, Ruschlikon, 2008.
- [44] European Commission, "eGovernment in Turkey" European Commission, 2016.
- [45] G. Gürkaynak and İ. Yılmaz, "Transition to national eID cards" *International Law Office IT & Internet Newsletter*, January 2015.
- [46] oauth 2.0, "oauth 2.0" 8 August 2019. [Online]. Available: <https://oauth.net/2/>.
- [47] tbb, "banka sube bilgileri" 8 August 2019. [Online]. Available: https://www.tbb.org.tr/modules/banka-bilgileri/banka_sube_bilgileri.asp.
- [48] eGovernment Innovation Center, "eGovernment Innovation Center" 8 August 2019. [Online]. Available: <httpswww.egiz.gv.aten>.
- [49] itu, "Expert Group Meeting on Mobile ID" 8 August 2019. [Online]. Available: <httpswww.itu.intenITU-DRegional-PresenceEuropePagesEvents2016mIDExpert-Group-Meeting-on-Mobile-ID.aspx>.
- [50] C. Rath, S. Roth, H. Bratko and T. Zefferer, "Encryption-Based Second Authentication Factor Solutions for Qualified Server-Side Signature Creation" *Institute for Applied Information Processing and Communications*, pp. 71-85, 2015.
- [51] C. Sullivan, "Digital Identity - From emergent legal concept to new reality" *Computer Law & Security Review*, vol. 34, pp. 723-731, 2018.
- [52] European Commission, "Digital Government Factsheet 2019 - Turkey" European Commission, 2019.
- [53] T. Martens, "Electronic identity management in Estonia between market and state governance" Tallinn: Springer, 2010, pp. 213-233.