INTEGRATION OF TURKISH EID WITH E-GOVERNMENT & E-BUSINESS SERVICES

Oktay Adalier
TÜBİTAK BİLGEM UEKAE, 41470, Kocaeli, Turkey

Mucahit Mutlugun
TÜBİTAK BİLGEM UEKAE, 41470, Kocaeli, Turkey

Ahmet Fatih Mustacoglu
TÜBİTAK BİLGEM UEKAE, 41470, Kocaeli, Turkey

─Abstract ─

eID cards and electronic authentication known as E-authentication are becoming more and more popular at Government and Business institutions for recent years and both concepts will continue to remain important for the next decade. Especially in Europe, almost all of the countries have an eID project and the level of the progress varies based on the countries. The citizens have gained great benefits from those e-Government Applications in terms of easy use of the services, and rapid return of the results. But there is a big issue from the service provider point of view. Since the resource which is shared by the service requester is very big and the eligibility of the requester is not easy to identify in electronic environments. The main necessity of the entire e-Government and e-Business system is to provide a common electronic authentication system that guaranties the eligibility of the service requester (citizen) of a service in an electronic environment is the right person. After stating the principles of Authentication, we introduce Turkish eID card and Electronic Authentication, System (EAS) respectively. We share the experiences that we have obtained during the pilot application of the projects. We discuss the abilities of reducing the bureaucracy in business services via the support of eID card and EAS. As a future work, we identify the requirements for a Turkish eID Integration Center for eID integration with e-Government and e-Business applications.

Key Words: *eID, Electronic Authentication, eServices.*

JEL Classification: H7 - State and Local Government

1. INTRODUCTION

eID cards and electronic authentication known as E-authentication are becoming more and more popular at Government and Business institutions for recent years and both concepts will continue to remain important for the next decade. Especially in Europe, almost all of the countries have an eID project and the level of the progress varies based on the countries. For instance, some of the countries have already finished the deployment of the projects, several of the countries are making pilot projects and the rest of the countries have a plan to prepare projects.

The main motivation for eID is transforming the business processes from classical environment into electronic ones through the e-Transform program. State Planning Organization (DPT) has started the Turkish e-Transform Program at 2006. The first 5 years of the program has been completed. There are more than 100 action-items to be implemented for several government institutions. At every action, the responsible institution conducts some research and effort to develop a huge e-Government application to convert its business services into services that run in electronic environment. Some of them can be listed as MERNİS, TAKBİS, UYAP and Government Portal.

The citizens have gained great benefits from those e-Government Applications in terms of easy use of the services, and rapid return of the results. But there is a big issue from the service provider point of view. Since the resource which is shared by the service requester is very big and the eligibility of the requester is not easy to identify in electronic environments. Due to the weak authentication in electronic environments, the economical size of unfair issuance of eServices exceeds an amount of 10 billion TL in each year.

The main necessity of the entire e-Government and e-Business system is to provide a common electronic authentication system that guaranties the eligibility of the service requester (citizen) of a service in an electronic environment is the right person.

With the motivation of Turkish Prime Ministry circler and under the sponsor of TUBİTAK TARAL program, the Turkish eID project has been developed and a pilot application has been established successfully at the city of Bolu. During the pilot project period, the Turkish Electronic Authentication System has been integrated successfully with several e-Government and e-Business applications.

In this paper, we present integration principles of Turkish eID with e-Government and e-Business services. Firstly, the current eID developments in the world, especially in Europe, are mentioned. After stating the principles of Authentication, we introduce Turkish eID card and Electronic Authentication, System (EAS) respectively. We share the experiences that we have obtained during the pilot application of the projects. In the next section, the principles of the integration process of eID with e-Applications are discussed in detail. Then in the following section, we represent case studies with examples from e-Government, e-Finance and e-Business applications. From e-Government point of view, we discuss the integration of MEDULA and Health Automation systems with the EAS including e-Receipt. In addition, we model the integration of Turkish Notary business system with EAS. On the finance domain, we discuss the integration of individual and institutional banking applications that use EAS infrastructure including ATM using of eID cards, while on the business domain, we give the integration of Turkish e-Government Portal as a key issue for business integration.

At the end of the paper, we discuss the abilities of reducing the bureaucracy in business services via the support of eID card and EAS. As a future work, we identify the requirements for a Turkish eID Integration Center for eID integration with e-Government and e-Business applications.

2. TURKISH EID AUTHENTICATION SYSTEM

2.1 The Infrastructure of Turksich Authentication

Architecture of the Turkish eID authentication system, its components and the flow of the authentication system are depicted in Figure1 below (Mutlugün, 2009):

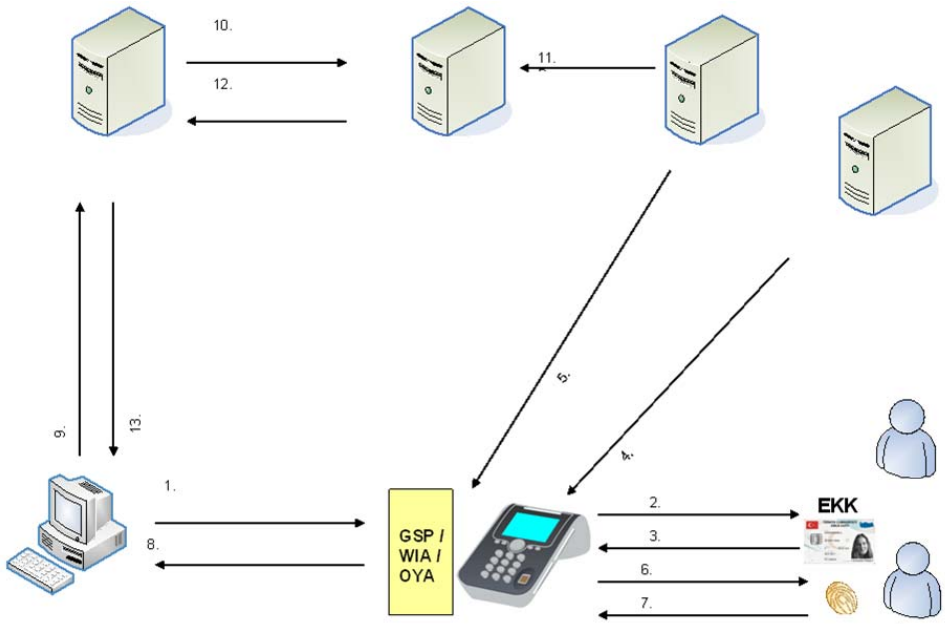

Figure1: Architecture of the Turkish eID Authentication System

In the proposed system,

Citizen → Claim owner

Finger print, PIN, ID, certificate → Proving units

ID Access Device → Authenticator

Institution Service System (Client / Server) → Trusting part

Institution Service Server

Above roles are defined. After having a citizen's request for having a service or accessing information, the Turkish eID Authentication steps that are using the eID Authentication System Components will be as follow:

1. Institution service client creates an eID Authentication request. Then, institution service client sends the prepared request to ID Access Device (IDAD) through the other sub-components called as Security Services Platform (SSP). SSP is explained in detail in section xxx. The client sends a request including authentication reason and its role tag (service requester/service participant) and role information for eID Authentication to SSP. Next, SSP sends the coming request to the related IDAD.
2. IDAD asks citizen for his/her ID card.
3. Depending on authentication role, the citizen inserts his/her card into the IDAD's related slot. Then, IDAD authenticate ID owner's unique id in the citizen's card by validating the signature.
4. SSP communicate with the predefined ID Authentication Policy Server (IDAPS) by using the ID Authentication Summary (IDAS). IDAS includes the rol and the Turkish Citizen Identification Number. Then, IDAPS prepares the policy data for the related application and the citizen. After that, IDAPS signs the policy data and send it to SSP. The most important variable in the policy data is the security level. SSP has the ability to hold policies in its cache and can use them until their expiration date. If SSP can not reach the IDAPS, then it notifies the IDAD resulting in the authentication level to be the highest.
5. To check the validity of the ID Authentication Certificate, SSP sends an OCSP request that is prepared by the IDAD to the Certificate Server. SSP sends the incoming OCSP result from the server to the IDAD. Based on the coming OCSP result (ID is cancelled or not), IDAD either terminate the process or continue to the process. If the SSP can not reach the OCSP, then it inform the IDAD and then IDAD continue to its process and includes that it can not reach the OCSP. Furthermore, SSP has the ability to move OCSP requests to its cache and reuse them if necessary.
6. IDAD requests the PIN/Finger Print based on the security level defined at the coming result from the IDAPS. In the case of security level 1 and 2 that only requires ID card, IDAD continue to process its job. The process is cancelled if the citizen can not provide the requested properties.
7. The citizen gives the requested PIN/Finger Print to IDAD.
8. After performing the authentication processes based on the requested security level, IDAD prepares ID Authentication Summary (IDAS) and sends it to SSP if the authentication is successful. IDAS is only signed by Security Access Modul (SAM) and ID Card if the security access level requires PIN. Otherwise, IDAS is only signed by SAM.
9. Institution Service Client (ISC) sends the IDAS to its own server.
10. Institution Service Server sends the IDAS to ID Authentication Server via secure channels.
11. ID Authentication Server checks the validity of the SAM's certificate that signed the IDAS by either using the Certificate Revocation List (CRL) or by sending a request to OCSP. ID Authentication Server checks the validity of the certificate by in the means of CRL or OCSP if IDAD did not checks the validity of the certificate.

12. ID Authentication Server executes the authentication process, saves the IDAS to database and sends the result to the Institution Service Server.
13. ID Authentication Server decides whether giving a permission to the requested service based on the authentication result and returns the decision to the Institution Service Client.

2.2 Turkish eID Components

2.2.1 eID Card

Turkish eID Card composed of the following components:

- Turkish Identification Number, name and certificate number that are signed by NVI.
- Electronically signed picture of the citizen
- Electronically signed finger print of the citizen
- eID Authentication certificate
- Electronically signed personal identification information

Turkish eID Card holds many physical properties for security and it also contains many other properties electronically for security as well. Operating system of the smart card has the Common Criteria EAL4+ and smart card chip has the Common Criteria EAL5+ security certificate. eID Authentication certificate located on the smart card is compatible with the X.509 standards.

2.2.2 ID Access Device

ID Access Device is used as an authentication tool in the Turkish eID Authentication System. It has also special module called as Security Access Module on it and its main duty is to authenticate the eID card. Security Access Module is responsible for cryptographic processes.

2.2.3 eID Authentication Server

eID Authentication Server is responsible for authenticating the ID Authentication Summary.

2.2.4 eID Authentication Policy Server

eID Authentication Policy Server is responsible for defining a policy for eID authentication.

2.2.5 eID Authentication Policy

eID Authentication policy is produced digitally by eID Authentication Policy Server, and it is constructed in ASN.1 structure. Its contents are as follow:

- eID Autentication Role
- Security Level
- Security level of the finger print
- Policy validity date
- Validty period of the ID authentication summary
- ID authentication condition

- Generic policy
- Permission for reusing the security level
- Permission of the mediator
- eID Authenticaion Server Certificate and signature

2.2.6 eID Authentication Sub-Components

eID authentication requests have to use eID Authentication sub-components in order to access ID Access Device. There are two types of sub-components:

- Secure Services Platform for ID Access Devices that are using ethernet interface
- OYA for ID Access Devices that are using USB interface.

2.2.7 eID Authentication Summary

The data that are generated in the eID Authentication Summary is given below:

eID Authentication Summary	**Sample**
Id	72334
eID Authentication Summary Version	1.00
Summary No	257
Card Serial No	PL3072420
TC No	22755391259
Name	MEHMET
Last Name	İNALTEKİN
Card Validty Date	19.11.2019
Is mediator used?	no
Mediator Card Serial No	---
Mediator TC No	---
Mediator Name	---
Mediator Last Name	---
Mediator Card Validity Date	---
Person who is a part of the authentication	no
Person who is a part of the authentication Card Serial No	---
Person who is a part of the authentication TC No	---
Person who is a part of the authentication Name	---
Person who is a part of the authentication Last Name	---
Person who is a part of the authentication Card Validity Date	---
Execution Sticker	hastaKabul@sgk.gov.tr
Execution Sticker Explanation	Patient Admission

Security Level	Level-3
Expiration Date	86400
Role	Service requester
Biometric Authentication Status	A/D
Device chasing No	16777449
Service Provider chasing No	1,0203E+14
SAM chasing No	3366001c91ff274fda141c15
Creation Date	08.01.2010 13:38
IDAD Driver Version	1.33.03
Is card cancellation checked?	yes
Institution No	
SAM Signature	
eID Card Signature	

3. CASE STUDIES OF INTEGRATION OF EID WITH ESERVICES

3.1. Integration EAS with Social Security System

MEDULA

In the current system, permission for a patient from Turkish Health Care System is obtained by TC Identification Number and this process is converted to use ID Authentication Summary instead of the TC Identification Number (Mutlugün, 2010). This process is executed as follow:

- A citizen goes to application point to get a service.
- The responsible person at the application desk uses Hospital Data Management System (HDMS) software to initiate the id authentication process.
- HDMS requests the id authentication from the SSP. HDMS sends hastaKabul@sgk.gov.tr execution sticker, role of the service requester and information for which IDAD to use. to SSP.
- SSP completes the id authentication process by using IDAD. During the id authentication, SSP obtains the policy from ID Authentication Policy Server belongs to Government Healthcare Institution. The security level at the policy is defined by the Government Healthcare Institution so that PIN and finger print is requested or not during the id authentication.
- SSP sends the ID Authentication Summary coming from IDAD to Government Healthcare Institution.
- Government Healthcare Institution calls the MEDULA web service by using ID Authentication Summary in order to identify the patient's eligibility.
- MEDULA uses ID Authentication Server to authenticate the coming ID Authentication Summary.

- MEDULA uses TC Identification Number coming from the ID Authentication Server to query the database in order to identify the eligibility of the patient. And returns the result to the Government Healthcare Institution.
- If the coming result from MEDULA is successfull then the patient is directed to the related doctor.

3.2. Integration EAS with Financial Services

The financial sector has an important place in Turkey. It leads to technological advancement in the everyday life. The online banking application is used by many customers and ATM are scattered around the country. Turkey has the third place within Europe continent by owning the credit and debits cards. The use of those cards exceeds billon of Euros yearly. Every Bank has its own online authentication system. The customers should memorize several passwords and access words for online banking system. On the other hand every online banking system has different authentication system. This situation makes the life for customers difficult and increases the maintenance of the system. Managing the debit cards is another problem for the banks. The Turkish ID card and Electronical Authentication System (EAS) eases the life for both sides. The customers use the national ID cards at ATM environments. For authentication the national EAS is used. For online banking environments the customers should own standard smartcard readers. From the home/office they can connect to the banking services by using national ID cards. After authentication by using EAS they can benefit from the services. As a result the customers should only know one PIN code and use a single eID card. It makes the life ease for both sides.

3.2. Integration of Turkish e-Government Portal

'e-Devlet Kapisi' is to be Turkey's first eGovernment gateway and is well under operation. The portal aims to provide Turkey's 70 million citizens with a single point of access to eGovernment services. Currently it support s more than 150 eServices which is owned from several governmental institutions. The gateway also serves a third group of users – the public sector agencies themselves – allowing them to interact with each other and exchange information.

There are for ways to enter to the portal. The first one is by using a username and password. Citizens can hold a username and password pair from post offices. But they very often lost the password. The second one is by using eSign certificate which is given by official certificate provider. This case is a little bit costly since the qualified certificate can be owned by paying some amount. The third one is by using Mobile Sign certificate. There are two cell phone operators in Turkey who give mobile eSigning support. It requires using cell phones to enter the portal. It also cost some amount of money. The last one is by using national eID card and a card reader. Figure - 2 shows the access window of Turkish Governmental Portal via eID.

Figure-2: Access window to Turkish Governmental Portal via eID

4. CONCLUSION

The integration of Turkish eID and EAS with eServices has reduced the complexity of authentication process. Reduce the maintenance cost. Simplify the use of authentication for user side. Increase the security and unify the infrastructure.

As a future work, we identify the requirements for a Turkish eID Integration Center for eID integration with e-Government and e-Business applications. There will be and authority for guiding the integration process with eService owner. System analyst support will be given those who have complex applications and process. There will be a testing team ready for qualifying the integration.

BIBLIOGRAPHY

M. Mutlugün, O. Adalıer (2009), "Turkish National Electronic Identity Card", International Conference on Security of Information Networks.

M. Mutlugün, O. Adalıer (2010), Turkish Authentication System Definitions Document.

Turkish eGovernment Portal via national eID (2011),
https://giris.turkiye.gov.tr/Giris3/ekkGiris?actionName=ekkGiris