SCALABLE ECOSYSTEM DEDICATED TO DIGITALIZATION OF CITIZEN-ADMINISTRATION INTERACTION

Ana Maria POPA (CHIRIAC)[1], Ştefan MOCANU[2]

Citizens in today's society have different needs and requirements in relation to the administrative entities they must interact with. Digitalization is a modern concept that involves the use of ICT techniques to facilitate interactions in the online environment, reducing or even eliminating traditional documents based on paper and pen. To achieve this goal, huge challenges must be addressed in what concerns security, digital identity, networking and others. This paper presents a fully functional system, already in use by several territorial administrative units in relation to citizens.

Keywords: digitalization, digital identity, digital signature, public administration

1. Introduction

The evolution of digital technologies has already started to revolutionize public administration in many countries of the world. For new technologies to be as efficient as possible, they must be accompanied by organizational changes and transparency regarding the use of digital public services by citizens and companies. At EU level, there are many initiatives that support local (national) and global (international) digitalization of various services to enhance cooperation in fields like economy, trade, health, education, and others. During the past years, European Commission has focused its attention on creating a single market through which free access to services and the free movement of people can be safely achieved without geographical borders or other barriers. A common and binding legislative framework has been established for all member countries, with each state having its own legislation based on the European one. For this to work, first it is necessary for all countries to move most public administration and government services into digital environment.

This study aims to support the need to invest in public administration digitalization. This process not only will improve transparency and efficiency of public services, but it will also make the process easier and faster for the citizen.

[1] PhD student, Dept. of Automatic Control and Industrial Informatics, University POLITEHNICA of Bucharest, Romania, e-mail: anamaria@ingenios.ro

[2] Associate professor, Dept. of Automatic Control and Industrial Informatics, University POLITEHNICA of Bucharest, Romania, e-mail: stefan.mocanu@upb.ro

The actual context, generated by the COVID-19 pandemic, is increasingly demonstrating the benefits of public services digitalization. Next step will be represented by connecting national services to similar ones from other European countries.

2. Related work

Studying several papers, we saw that in France [1] the first digital services appeared in 1996, but they were services to promote the activity of the government, so essentially political instruments. In 1997, the first public services appeared online, after which "AdmiFrance" was launched, the first administrative site that, in addition to providing information, allowed users to download administrative forms. In a ranking dedicated to e-government, France is on the first place; in 2014 it was first in Europe and fourth in the world according to the E-Government Development Index (EGDI). This classification is made considering three directions: the provision of online services, telecommunications infrastructure, and human capital. In 2015, the European Commission made a different ranking based on 30 indicators divided into five sectors: connectivity, digital skills, online activities, integration of digital technology by companies and digital public services. According to this ranking, France is on the 14th place in Europe, above the European average but quite low compared to the leading country in the digital administration of Estonia. Estonia has been a pioneer in transforming public services into flexible electronic solutions for citizens and e-residents. Estonian public institutions have gradually transitioned from the old existing systems to the new Government Cloud solution, which has been developed in accordance with the national IT Security Standard (ISKE) [13].

In Germany, the e-government regulation was introduced on 1 August 2014 [2]. This "Digital Administration 2020" regulation provides deadlines for electronic access for individuals, companies, and public administration. This program pays special attention to modern technologies, makes legal and organizational changes, and analyzes ideas and suggestions from companies and individuals.

In [3], the authors present the form of e-government in Indonesia as a reform of public administration. This digitalization has reduced faulty administration and direct contact between service providers and service users. Although direct contact has been diminished and many electronic services are provided, it has been recognized that not all types of public services can be provided entirely electronically. The researchers relied on a descriptive method and a qualitative approach through discussions with stakeholders and service providers. Along with this reform, the most difficult challenge remains to keep IT up to date. That is why the authors recommend that all regional units be updated

immediately and that the direct contract between service providers and service users no longer exist and that services to the community be continuously improved.

The country that has best achieved its goal of digitalizing public administration is Denmark, as presented in paper [4]. The authors claim that Denmark, followed by Sweden, Finland and the Netherlands, forms the group of countries that perform best in digitalization in the world.

The level of decentralization of Danish public sector together with the division of public administration into three levels, state, regions, and municipalities made possible the implementation of e-government easier because reducing the number of regions and municipalities has simplified political structure and increased the budget for each municipality and region.

In a study conducted in Portugal [5], the authors argue that digital government or e-government is a field of research consisting of several disciplines such as public administration, knowledge management and innovation, management of elements and processes, information technology, communication and organizational culture. This article focused on how the process of digital transformation in public administration takes place and the relationship with knowledge management. A better understanding of knowledge management could provide an eloquent strategy for managing digitized content that is as easy to use and accessible as possible and to keep it up to date.

The authors of the paper [6] reached three main conclusions for reforms in the administrative sector. The first conclusion says that the efforts needed to reform the public sector must be context sensitive and follow various approaches. No model of one country is entirely fit to solve the problems in the administrative system of another. The second conclusion is that those who will be able to experience the new will be those who have established the basic organizational requirements of a functional administrative public. The third conclusion refers to the heterodox approach on a series of public management that will be more suitable for many developing countries than the approach of models that have formed in the political and economic conditions of some heavy industrialized countries.

In paper [7] the author presents the evolution of e-government and the connection with public administration in United States of America. He made an analogy with e-commerce covering four areas common to government and public administration: citizen and state relations, domestic operations, social and economic programs, and the relationship with the international environment. The emergence and evolution of e-government has influenced public administration in the last ten years, especially in developing countries. The citizen-centered service argues that it is the strongest concept of electoral governance from this point of view, the services must start from satisfying the needs of the citizens, helping the

citizen to fulfill his civic obligations. Information as a public resource of public administration represents the emergence of information as a government resource. The information gathered for one purpose can be used for other purposes, creating significant possibilities but also related problems. The third feature of e-government is the technology that shapes the environment in which public administration operates. For the management side, technology has been a major challenge for managers called upon to make decisions on the investment side in a rather complex IT system. In each of these areas characterized above, developing countries face limitations on infrastructure, financial resources and low levels of development.

A research on e-government in South Korea presented in paper [8] shows that government officials' satisfaction with the digitalization of administrative systems will increase when the systems are easy to use, useful and produce high-quality information. Likewise, citizens will be satisfied with these services when officials use these systems to meet their needs and provide secure and reliable information and services.

The authors of the paper [9], after analyzing digitalization and how services can influence the adoption of the Internet, in countries such as Germany, South Korea and the United States argue that success in digitizing governance and public administration resides in building a strong foundation for a wide range of online users, creating deep and varied content, generating mechanisms to support online advertising and payments and building a solid environment for companies to invest in online commerce and services. If all these services are put into operation, the whole ecosystem of digital services will work and will be able to become self-sustaining.

The authors of paper [10] claim that for a successful/reliable digitalization, the states must follow two main directions. First is to develop strategies for the specialization of those without higher education, with the basic software for a good evolution at work. After years of digitization, basic knowledge of Microsoft Office and other day-to-day programs is a prerequisite for joining the mass economy. Second, states need to train or seek IT specialists, knowing that the digitization process will continue to expand and the need for IT professionals will be growing not only in IT specific industry but also in most economic sectors.

Digital Single Market has included several European Directives and Regulations, the most important being GDPR (General Data Protection Regulation) - eIDAS (European Union's Electronic Identification and Trust Services Regulation) - Regulation on the provision of electronic identity, electronic signature, electronic seal and time stamp and PSD 2 (Payment services Directive (EU) 2015/2366) - Directive on payment services in the common market. The eIDAS regulation contained a legislative framework for cross-border

access to services and the secure making of online payments by individuals and organizations belonging to EU Member States [11].

When it comes to digitalization an important aspect is represented by digital identity. A real problem nowadays is finding a solution that is as reliable and secure as possible for remote identification mechanisms. The user-password solution is no longer satisfactory, especially when it comes to e-banking, local public administration, or government applications. As we have seen in many papers, most states have a solution, but the lack of compatibility and interoperability is why a regulation is needed to provide a unitary framework for secure interactions between citizens and administrative entities [12].

3. Proposed system

Digitalization is a necessity to which we would like to contribute to with a concept of open architecture system based on an ecosystem comprised of the components depicted in Fig 1.

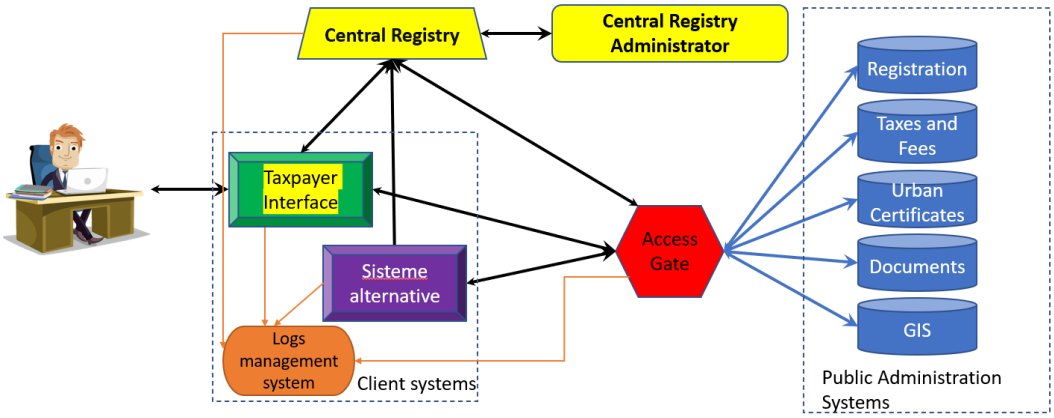

Fig 1. Ecosystem architecture for digitalization of public administrations

These components will allow implementation and scaling at any national level of interaction between the citizens and Public Administration systems and have the following meaning:

i. Central Registry – is a virtual dispatcher answering to requests such as:
   - Presentation page specific for human visualization
   - Internet address for online accessible systems through computer-based interface
   - Records for recommended trust services
   - Available services for each accessible instance.

- Support for forms catalogues
- Status and/or log concentrator (future plan)

ii. Central Registry Administrator – responsible for:
- Configuration interface for the specific settings of the Central Registry
- Initially it will work as a unique location, but it can be organized for multiple interfaces, for cluster management (in the future)
- Dynamic Forms Manager - creation and distribution towards systems that can support this mechanism

iii. Client Systems – available2 at client's end
- Manage customer registration (usually they are taxpayers for local public administration)
- Make digital identity security checks (check the validity of user certificates through OCSP)
- Manage form requests (initiation, adding files, generating reports in legal format, messaging, status management, access management)
- They can be simple web systems, mobile applications or third party systems/ specialized ERPs
-

iv. Access Gate systems - are connected to the internal systems of the Public Administration
- Manage all access points from the internet, validating the structure according to the Central Register
- Ensures security checks of requests from client systems
- Ensures guiding and possibly moving the requests towards the systems that are responsible to respond (for example - registry, taxes, urbanism, document management, GIS, etc.))
- The implementation function can ensure the interface for full or partial validation of requests before sending them to the internal systems, using the integration of access rights from the existing systems
- Digitally sign the output documents using the electronic seal in several forms (local electronically, on a secure stick or in cloud)
- Ensures traceability and log tracking interface

v. Specific Systems of Public Administration
   - Direct access through database, through the file structure (eg FTP) or through web services
   - Require adaptations to respond to online systems, but it frees up responsibilities such as structure verification, security and complex traceability

3.1 Functional description

In this ecosystem the focus was set on the mechanism dedicated to securing the authentication and authorization process, trying to prepare the ground for the infrastructure to be compatible with the EIDAS changes that will be activated soon. The current poor legislative support is likely to have numerous updates that will require specific changes that we will be able to integrate easily in the structures created.

The enrollment process treats the following elements independently, carefully and in the client interface:

1. Access credentials – at the beginning this is based on an email address and a password
2. The system operator - the identification details and the supporting documents are introduced
3. Represented person - enter the details of the represented person and supporting documents. The represented person can be:
   a. The natural person
   b. A person represented by another person,
   c. Legal entity (SRL, SA, CA, Notary, PFA, II, NGO, etc)
4. Institution to which they enroll - selected from the available list. Depending on the needs, specific interests can be added to the contractual enrollment relationship - for example, a notary should be able to request.

At the end of the enrollment process, a predefined standard contract is generated, which specifies the collaboration conditions and the value of an implicitly agreed contract, automatically generated from the system based on a preconfigured template. The gateway receives the request from the client interface and further delegates the validation process to a specific interface and then to a responsible human operator. He will check the elements mentioned in the attached documents, and depending on the details being valid or not, he will confirm or reject the enrollment request. In the close future, when the EIDAS protocol will be active, this enrollment process will no longer be necessary, as it will already be validated by the identity operator. Depending on the settings in the system,

validation mechanisms can be defined to be conditioned by the digital signing of the documents in the system and implicitly the automatic validation of the digital certificates used for signature, through specific online digital certificate mechanisms (OCSP). Email notifications are automatically integrated into system feeds for each decision change status message or messages with specific questions from one of the parties in the dialogue.

The actual solution is mainly focused on the Romanian public administration; therefore, we have implicitly built a series of functionalities optimized for these local tax systems:

• Request for issuing a fiscal certificate, with the possibility of online verification in a secure way (can be done only by persons authenticated in the system, valid GDPR)
• Car registration request
• Request for registration of buildings and land

3.2 Dynamic forms

For general forms, based on a simple structure or on attached documents we have designed an infrastructure to create interactive flow of forms that can be defined according to customer needs, using the infrastructure of security, digital identity, representation, messaging, and notification just like in the case of statically defined forms. As soon as the infrastructure is installed, forms can be defined as follows:

- A system administrator defines a form , with a dynamic structure, within the Central Register
- The designed form is installed on the support system of the Access Gate and is accessible on its validation interface
- Once installed on the support system of the Access Gate, it will be accessible by the Client Systems that are accepted by the Access Gate, to communicate completed forms and to support the takeover and the answer.

An example of such a flow is the application for a town planning certificate. The form contains only a few text fields, some documents must be attached, notifications must be sent when it has been submitted, when it has been processed, when the file has been checked, etc. But most importantly, the details of the person who made the request must be checked so that confidential resources cannot be accessed by people who are not allowed to do so - for this we have a standard flow of validation and secure response. All elements for this flow are created by following the steps above.

3.3 Cascading services

The presented system can allow the delegation of requests between computer systems that trust each other. Thus, similar elements of forms can be cascaded to allow a request to one institution to automatically obtain answers from other institutions. This can only be done on a reliable relationship between computer systems, this is preferable to be done with a secure service infrastructure, based on electronic seal for each system, and all requests and answers can be verified based on these seals. A practical example is the registration of a car at DRPCIV (Romanian authority for issuing driving licenses and car registrations) which can automatically request the deregistration of the vehicle from the seller's TAU (Territorial Administrative Unit) and the registration to the buyer's TAU, as one can see in Fig 2.

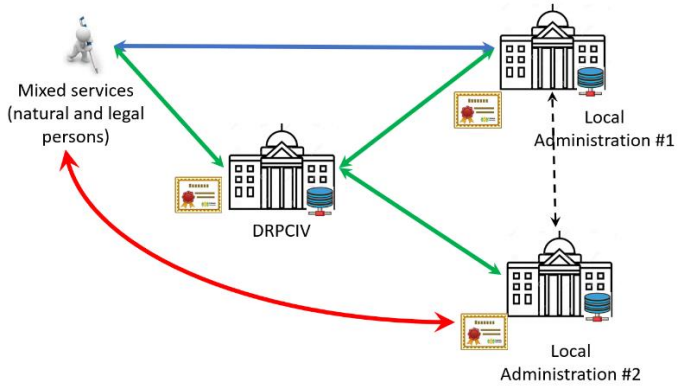

Fig 2. Cascade services

Starting with March this year, due to the COVID-19 pandemic and the imposed self-isolation, Romanian authorities and public institutions are obliged to accept documents signed with electronic signature, sent online by companies and individuals. According to the normative act, the electronic signature and the electronic documents can be used at the level of public authorities and institutions. Documents issued in electronic format by public authorities and institutions will be signed with a qualified electronic signature and will be assimilated to official documents, as they are defined by law.

Furthermore, starting with the date the normative act became effective, public authorities and institutions have the obligation to electronically receive signed documents, and each institution will determine the type of electronic signature applicable for use by individuals or legal entities of a service available online and provided by that authority / institution. Until March 2020, although our system performed the digital identity security checks at the time of enrollment and when submitting any application, in order to be accepted in the system the taxpayer had to travel at least once at the mayor's office to physically sign an

agreement that stated that the connection with the authority will be done using the online environment as well. One can ask a legitimate question, that is Why ? Unfortunately, because there is no online mechanism to corelate the digital certificate from the identity provider and the personal numerical code of the holder. To make it clearer, in case of two people with the same name, if one signed the document for the other, than that person could access the system without difficulty, causing a serious security issue.

To avoid any problems when people who have a digital identity from an accredited identity provider are accessing the system, we have implemented a new access concept through which the accredited digital identity provider certifies the person's online identity. This new concept has two flows, one for enrolling a new taxpayer who owns a digital certificate and who needs to create a new account in our application to manage the relation with the mayor's office and another flow that requires only validation of the taxpayer who is enrolled in both systems. An example of a flow for creating a new account presented in Fig. 3a while the flow for a person who owns a digital certificate is presented in Fig. 3b

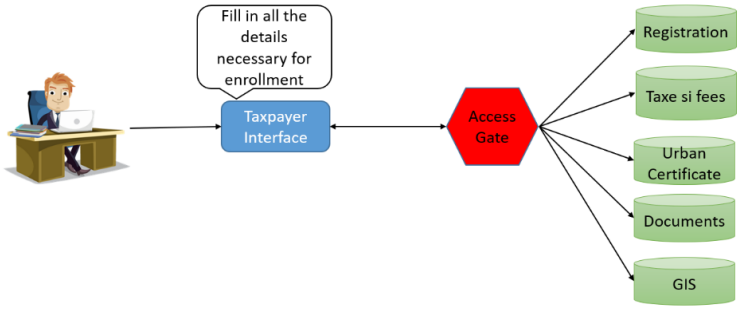

Fig 3a. Local authentication

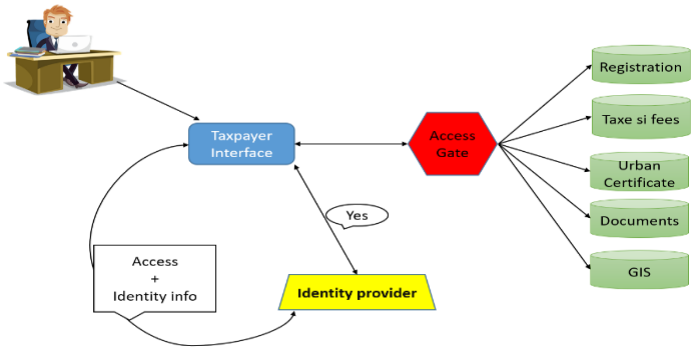

Fig 3b. Authentication using the identity from the Identity Provider system

The user accesses our application, on the login page he is asked *Who knows you*? If the user has a digital identity certificate, he will select the provider of his certificate from a list and will then be redirected to the provider's authentication page. After authentication, he will return to the application where he will complete only steps 2 and 3 of enrollment, steps that refer to which person he wants to represent (own person, a legal person, or another natural person) and in step 3 he will select the institution that he wants to connect to and will upload the supporting documents for each case. Once returned to the user's application, the personal data coming over a secure channel from the identity provider will be filled in automatically; in addition to these data, he will also receive an identification code that will be verified each time he accesses the system. If in the second enrollment step the user selects his own person, he will be given automatic access in the system/application (he will have access to the menu for fiscal certificate requests, car declarations and real estate declarations and other statements made dynamically for each institution). If the user fills in other data than his own, then the taxpayer sends the access request to the mayor's office, a request that will be signed with his digital signature and will wait for an inspector to allow him access after analyzing the request. If the user does not have a digital signature he will follow and complete all enrollment steps, will send the request to the mayor's office, and will wait for an inspector to verify his data and then receive access to the application. The activity flow is depicted in Fig 4, but only details related to Fiscal Certificate issuance are provided due to the lack of space.

After creating the account using this flow, for other future accesses of the application, the taxpayer will repeat the steps with the digital identity provider, but over the secured service only the access code will be verified and then he will receive access to our application.

4. Results and discussions

The proposed solution to rely on remote authentication from the digital certificate provider's system instead of relying on local authentication presents several advantages. One of the most important resides in standardization, which means that authentication complies every time with national and international security rules and protocols. In addition, personal data checks are performed by a specialized system, not by a human operator which is not trained nor qualified to deal with such tasks and can make mistakes. For example, there was a situation in which a taxpayer uploaded his identity card in the system but, as personal data, he introduced his wife personal identification code (CNP). The inspector did not observe this simple mistake and approved the account, which granted the taxpayer to the system.

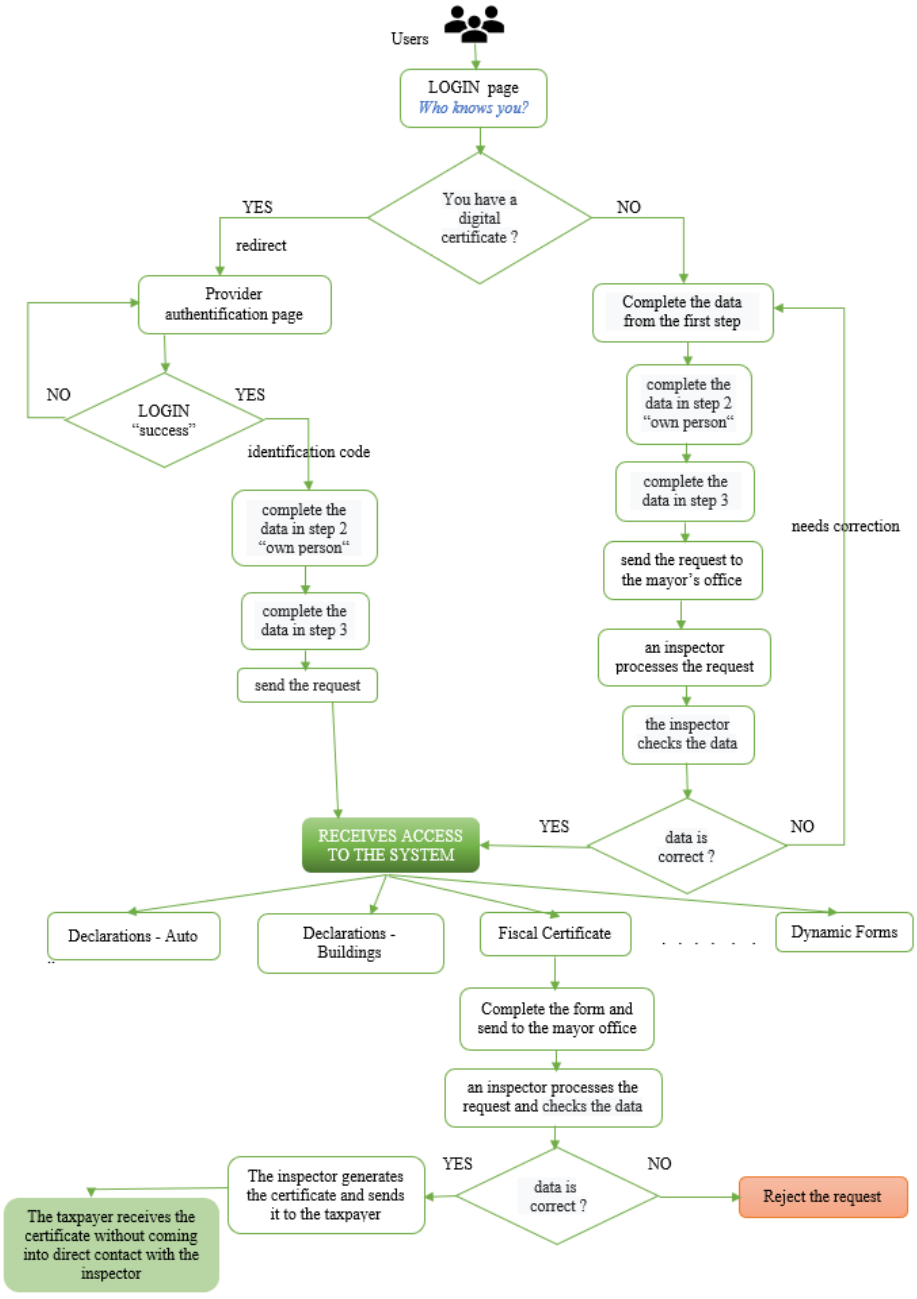

Fig 4. Activity flow for a simple interaction scenario between citizen and public administration

An important aspect is related to costs. By using the proposed solution, the financial costs of the system are reduced. From the user's perspective, a serious

decrease in access and use times is observed. Local authentication-based solution involved several interactions between the end-user and the mayor's office which could lead to access times situated between hours and even days. By using the proposed system, the access time is reduced to 5-10 minutes.

Another advantage worth mentioning is given by logging system. The traceability of the actions performed by the taxpayer at the time of authentication is double checked both by the logs from our system and by the logs from the other system. This way it is easy to identify any problems and to settle possible disputes.

During the implementation, several challenges had to be addressed. Once the number of users increased, the system had to able to scale up. For this reason, the database was very meticulously designed and optimized. A problem that had to be fixed came from the need of using digital signatures for signing the documents. For this to work, we needed the certificate verification service (OCSP) which, at the beginning of the implementation, did not function very well. The issue was fixed by working together with the certificate providers to make the service fully operational.

5. Conclusions

This paper presents the architecture and functional details of a system dedicated to digitalizing interactions between citizens and various administrative entities. Real life test revealed considerable reductions in time for the end user. This, along other advantages such as standard authentication procedures, hardware and software cost reductions, user action traceability, ease of use etc. validate the proposed solution. Details about the advantages of using our system can be found in section 4.

Acknowledgment

The work has been funded by the Operational Programme Human Capital of the Ministry of European Funds through the Financial Agreement 51675/09.07.2019, SMIS code 125125.

R E F E R E N C E S

[1]. Yann Algan, Maya Bacache-Beauvallet, Anne Perrot, Digital administration, Notes du conseil d'analyse économique, ISSN : 2270-2385, Volume 34, Issue 7, 2016, pp. 1-12

[2]. Die Bundesregierung, Digital Administration 2020 - Government programme of the 18th legislative term, https://www.verwaltung-innovativ.de/SharedDocs/Publikationen/Regierungsprogramm/management_summary_DiV_Druckversion_engl.pdf?__blob=publicationFile&v=2

[3]. Mila Viendyasari, The Application of Digital Administration to Minimize Maladministration in Public Services: A Case Study of Jakarta Investment and One Stop Service Department, Proceedings of the 3rd International Conference on Vocational Higher Education (ICVHE 2018), ISSN 2352-5398, DOI https://doi.org/10.2991/assehr.k.200331.133

[4]. Ada Scupola, Digital Transformation of Public Administration Services in Denmark: A Process Tracing Case Study, 2019, Journal of NBICT, Vol. 1, 261–284. doi: 10.13052/nbjict1902-097X.2018.014

[5]. Ana Alvarenga, Florinda Matos, Radu Godina and João C. O. Matias, Digital Transformation and Knowledge Management in the Public Sector, *Sustainability* 2020, *12*(14), 5824; https://doi.org/10.3390/su12145824

[6]. Mark Robinson, From Old Public Administration to the New Public Service - Implications for Public Sector Reform in Developing Countries, 2015, Public Sector Reform, https://www.undp.org/content/dam/undp/library/capacity-development/English/Singapore%20Centre/PS-Reform_Paper.pdf

[7]. David Brown, Electronic government and public administration, International Review of Administrative Sciences, Vol 71(2):241–254, DOI:10.1177/0020852305053883

[8]. Tina George Karippacheril, Soonhee Kim, Robert P. Beschel Jr., and Changyong Choi, Eds., Bringing Government into the 21st Century - The Korean Digital Governance Experience, 2016, ISBN (electronic): 978-1-4648-0882-1, DOI: 10.1596/978-1-4648-0881-4

[9]. Bahjat El-Darwiche, Mathias Herzog, Milind Singh, Rami Maalouf, Wissam Abourizk, Understanding digital content and services ecosystems - The role of content and services in boosting Internet, 2016, Strategy&, PWC.com

[10]. Mark Muro, Sifan Liu, Jacob Whiton, and Siddharth Kulkarni, Digitalization and the American workforce, 2017, https://www.brookings.edu/wp-content/uploads/2017/11/mpp_2017nov15_digitalization_full_report.pdf

[11]. Ana Maria CHIRIAC, Andrei Lucian LĂCĂTUŞU, Servicii de identitate digitală premergătoare implementării regulamentului eIDAS (Digital identity services prior to eIDAS Regulation implementation), Revista Română de Informatică şi Automatică (Romanian Journal of Information Technology and Automatic Control), ISSN 1220-1758, vol. 29(1), pp. 51-58, 2019. https://doi.org/10.33436/v29i1y201905

[12]. Ana M Chiriac, Andrei Lăcătuşu, Cosmin Popa, Ştefan Mocanu, Radu Dobrescu, "On Migrating from Present Identity Management Services to EIDAS", International Workshop on Service Orientation in Holonic and Multi-Agent Manufacturing, SOHOMA 2018, Springer, Cham, pp. 211-221, ISSN: 1860-949X,

[13]. M. Kitsing, "The Road Not Taken: From Digital Networks to Networked Governance," *2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS)*, 2019, pp. 457-462, doi: 10.1109/CCOMS.2019.8821720.