ENABLING RELIABLE, INTEROPERABLE AND SECURE E-GOVERNMENT SERVICES IN CROATIA

Martin Žagar[1], Josip Knezović[2] and Branko Mihaljević[3]

DOI: 10.24989/ocg.v335.24

Abstract
In accordance with the Croatian Government Decree on starting an e-Citizen project, National Identification and Authentication System (NIAS) was identified as a key enabling factor for the development of user-oriented public electronic services. Its role is to manage the identities in the electronic government ecosystem in the Republic of Croatia. Furthermore, NIAS is responsible for authentication of entities which access common system and the exchange of identity information between entities that communicate with each other through a common system, or exchange documents and data as well as verifying the authenticity of such identities. NIAS provides a credible general framework of trust and identity management which greatly simplifies the necessary infrastructure, organization, and services with significantly reduced costs for all stakeholders. In this paper, we will provide design and security details of NIAS as a basis for reliable, interoperable and secure e-government services in the Republic of Croatia.

Keywords: *electronic government, electronic identity, authentication and authorization system*

1. Introduction

In June 2010 Croatian Government started the procedure for defining the National Identification and Authentication System (NIAS) as a shared resource and building component of the national system to support interoperability among government entities involved in providing digital services. In practice, this meant that all activities related to the definition, establishment, and development had to be the result of coordinated national priorities and goals, and their implementation had to be managed and coordinated at the level of the national system. The action that followed was Croatian Government Decree on starting an e-Citizen project in April 2013. With this Decree basic public sector ICT infrastructure and framework for the development of user-oriented public services was set: Central government portal, National Identification, and Authentication System and Personal User Box System.

Similar concepts have already been realized in other countries worldwide as well. For example, Sweden has a national intranet network for secure communication between government bodies and EU bodies as a part of e-Government service [5], the Czech Republic offers citizens communication with the national authorities at one universal office, where you can receive or verify documents or acts from different institutions of public administration [1], Austrian Citizen Card can be used to sign documents electronically [3], Estonia first implemented X-Road infrastructure for cross-border

[1] RIT Croatia, D. Tomljanovića Gavrana 15, 10000 Zagreb, Croatia, martin.zagar@rit.edu www.croatia.rit.edu
[2] University of Zagreb, FER, Unska 3, 10000 Zagreb, Croatia, josip.knezovic@fer.hr www.fer.hr
[3] RIT Croatia, D. Tomljanovića Gavrana 15, 10000 Zagreb, Croatia, branko.mihaljevic@croatia.rit.edu www.croatia.rit.edu

services in domains not covered by existing EU and regional initiatives [8], Government Gateway in Great Britain enables people to communicate and make transactions with government from a single point of entry [2], VANguard is an Australian government program that delivers cost-effective and reliable authentication services to secure business to government and government to government online transactions [7]. In Croatia, NIAS is designed on the principles of the EU project STORK (Secure Identity Across Borders Lined), respecting existing practices and accepted standards, so the electronic connectivity with EU member states can be established in the simplest and most effective possible way [4].

This paper describes the model of central authentication and authorization system NIAS to clarify the legal powers of action-based allocation and use of resources in e-Government in the Republic of Croatia. In 2010 Croatia was on the 35th in the world e-government rank, and four years later, has progressed for five places [6]. In the group with the other countries of southern Europe is in third place behind Spain and Slovenia, just in front of Italy and Portugal, but in a group of post-conflict countries holding the first place out of 33 countries. It is followed by Georgia, El Salvador, Bosnia and Herzegovina, Lebanon and Azerbaijan.

UN explains how to post-conflict situations linked to weak and fragile states where the judiciary and the government are ineffective and where there is no provision of services. Post-conflict states are countries on whose territory fought a war over the last few decades [6]. UN study has shown that these countries have made significant progress with a decentralized integrated organizational model of e-government. This new approach supports the strengthening of institutional links between different departments and sectors; greater effectiveness and efficiency of the control systems and better public services.

Of course, the efforts in Croatian e-government at all levels is still affected by the lack of integrated administrative simplification and plan of e-government development, lack of infrastructure and human resource capacity, as well as the gap between supply and demand of e-services. Croatia as a country of low income continues to fight with traditionally limited investments in information and communication technology and the lack of technical knowledge, high prices of technology and inefficient government regulation.

According to that background, main goals that are set to NIAS can be briefly summarized as:

- Oversight of spending billions of HRK from the budget for ICT projects
- Creation of a unified database of all citizens, craftsmen, companies, associations
- Savings through better use of ICT infrastructure
- Introduction of a unified operation mode in all state bodies
- Online and single sign-on communication with citizens and companies through standardized processes.

2. Position, Roles and Relationships of NIAS

A high-level position and relationship of NIAS in the Croatian eGovernment framework is illustrated in Figure 1. End users access the system through the Users portal which aggregates all

the available services. The communication is performed over Government Service Bus or GSB which goal is to provide all the necessary infrastructure to exchange the data among framework entities such as government service providers, public or private data registers, external services etc. NIAS represents the first point of access, whether it manages the registration process or the authentication process. Registration process entails the initial procedure of the user's electronic identity creation. The authentication process is the first step in any subsequent user access to the system in order to consume the service.

The model of the NIAS system as the identification and authentication entity consistently supports the establishment and enforcement of the authorization rules in the system that is left for the service providers to define depending on the sensitivity of the data. In this way NIAS as a supplier and verifier of identities in the electronic government and the other participants in the system with their authorization policies complement each other in a comprehensive authentication - authorization architecture at the national level, with the specific goal of achieving a high level of interoperability and reusability tackling the ever-existing problem of data redundancy and synchronization.

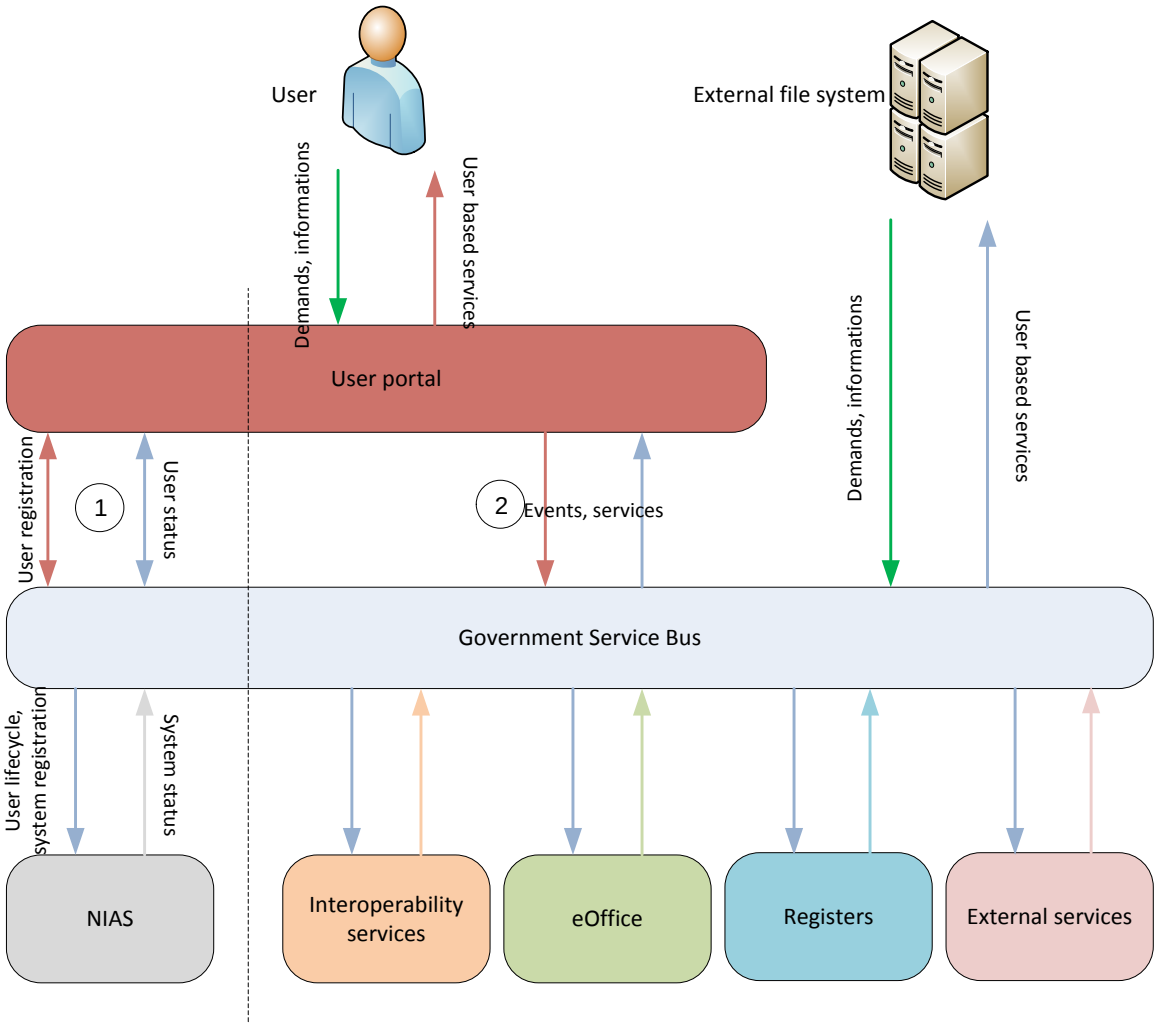

Figure 1. Relationship of NIAS to other building components of Croatian e-Government Initiative

2.1. Electronic Identity Elements

In order for citizens or business representatives to use electronic services, it is necessary to define appropriate elements and mechanisms to enable reliable remote identification. In digital world these mechanisms are known as processes to establish and allocate electronic identity to a real person, system, application, or service, which is then further used in the authentication process when the system checks to see if the other party is really who he/she says he/she is, as well as in the process of authorization when the system checks whether the user has the necessary privileges to perform some action.

Typical everyday examples of mentioned scenarios are the situations where a person uses the Internet, e-mail, mobile phone or similar to access specific information or electronic service. If the owner of the system allows its e-services to be used only by entities which are registered with him and he has awarded the appropriate authorization rights, he needs to establish the electronic identity management subsystem as part of its e-service system. Identity management checks the client identity and whether he/she has the necessary rights (authorization) prior to the use of the services. As a matter of fact, both parties must reliably determine who the other party is.

In the electronic administration, as the term is representing a connected back-office system of public administration, a user (person or business entity) should be given a possibility to have single electronic identity for all public electronic services instead of a myriad of various electronic credentials provided from every single public institution (or point of access), or even worse, from every single public electronic service. So, instead of every single public institution having established their own mechanisms for determining or verifying an electronic identity, a common central system should be built to manage all the data about electronic identities of people in the ecosystem of e-Government services. Such a system is represented by a trusted third-party component in the overall electronic communication framework between the participants in the transactions of e-Government.

Electronic identity in the e-Government presents a unique set of identification information about a particular entity (either persons or legal entities), which are maintained in electronic form and on the basis of which it is possible to unambiguously determine the identity to whom the data belong. Collecting and recording these data is performed by the predetermined and legally entitled institution(s) through the initial application process of registration in which the authorized officer must physically identify the potential user. The user is enrolled, and possibly further steps are performed in order to obtain additional security modules. Once enrolled, the user's data are then protected from unauthorized changing and updating. Registered entities can then use the given credentials for electronic communication in all processes that require electronic verification of identity in the concordance of the credential strength (security level).

The basic and mandatory element of electronic identity (e-ID) in the electronic government in the Republic of Croatia is Personal Identification Number (PIN), also abbreviated as OIB, as the unique identifier of the entity. OIB or PIN is a unique and universal identification number assigned to each physical or legal entity in the Republic of Croatia. It is administered and managed by the Ministry of Finance, Tax Administration. It is composed of 11 random digits devoid from any private or personal data such as gender, date, and place of birth etc. PIN/OIB provides uniqueness capability and reliable identification of users of electronic government in Croatia. Combined with optional Entity Name, PIN provides the starting point of a single electronic identity in the e-Government in the Republic of Croatia, as shown in Table 1.

This basic e-ID can be expanded with optional attributes such as surname, passwords, electronic box address etc. This set of attributes could optionally be expanded to include additional attributes that connect basic e-ID with additional information needed for example to prove the identity on the higher security levels (higher level credentials).

Basic identity element	e-ID – PIN number
An extensible set of optional attributes	Entity Name
	Entity (Personal) Surname
	Password (Authentication credential for security level 1)
	User Info box
	Mobile phone

Table 1. Basic electronic identity element and extensible set of optional attributes of electronic identity in the system of e-Government in Croatia

Service providers (government bodies, local bodies) that use NIAS may wish to extend the basic set of attributes of electronic identity provided by NIAS with additional, specific attributes which will be operated under their realm (jurisdiction) for the purpose of achieving the authorization policy at the local level. Additional attributes required for authentication at higher security levels by external credential providers (credential partners) can also be assigned to entity e-ID.

Likewise, the definition of the required security levels, authorization policies and the role of provided services are in the jurisdiction of service providers rather than NIAS. The role of NIAS is a safe delivery and validity of electronic identity authentication attributes. Basic e-ID in the e-government, together with a set of attributes from Table 1 is the responsibility of NIAS and provides proof of identity at the basic security level (Security Level 1).

The existence of a central directory of entities within NIAS represents one of the essential prerequisites for basic operations provided by NIAS. This directory does not explicitly exclude the existence of localized directories in the administrative bodies containing the connection of identities, their local roles or additional attributes of entities (such as employees) through which they cooperate with NIAS Central entity directory infrastructure established at NIAS contains a basic set of attributes required for the functionality of an electronic identity on the basic security level.

NIAS also provides and specifies mechanisms for expansion of the data set for the purpose of achieving higher security levels. All other attributes that serve as a base to establish authorization authority (roles, attributes related to positions, etc.) are the responsibility of the body that owns that data or provides electronic services, in compliance with policies and regulations set by NIAS.

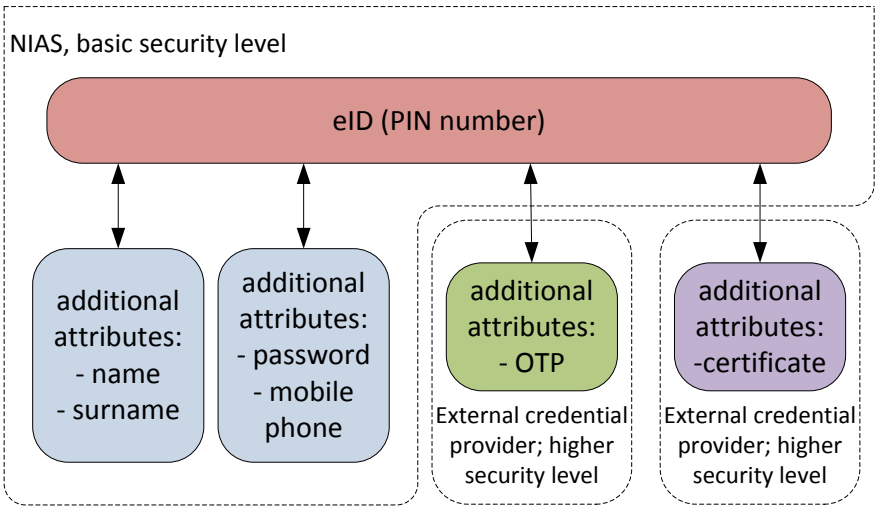

Figure 2. Organization of the elements of electronic identity system of e-Government in Croatia

Figure 2 shows the basic organization of electronic identity in the system of e-Government in Croatia. The basic data set (PIN/OIB number) forms the base on which to build additional attributes needed for multiple security levels. Creation of basic electronic identity, linking with the Tax Administration System that generates PIN/OIB, maintenance and deactivation of the identity is in the jurisdiction of NIAS. Additional information for electronic identity such as username/password allows the use of e-ID at the basic security level (security level 1 as will be described shortly). This data are under the authority of a NIAS as well. It is necessary to emphasize the following:

- Higher security levels and their corresponding additional data that may constitute electronic identity are optional and outside the jurisdiction of the NIAS (in the jurisdiction of external credential providers which have established partner relation to NIAS, i.e. electronic contracts). NIAS provides its association with its basic electronic identity. The external credential provider can be any other object that is by NIAS accepted as valid (partner relation).

- NIAS manages unique electronic identity management and the basic credential attributes required to achieve the basic security level.

3. Electronic Identity Registration and Operation

NIAS is designed with the goal to be flexible enough to allow interoperability and exchange of basic and specific attributes of the users of the system in order to provide electronic services (government bodies, local bodies, organizations) or define a relationship of trust in order to reduce unnecessary redundancy, i.e. increase the efficiency of the system.

Figure 3 depicts the scenario of the use of electronic identity:

1. User (citizen, company representative, an official in the administrative body) accesses the unified entry point through the government portal in order to achieve e-services.

2. To prove his identity, request for verification of identity shall be forwarded to the NIAS system.

3. If the required security level for the specified service level is equal to the security level 1 managed by NIAS, NIAS system will perform electronic verification of credentials. If the required security level is higher than 1, NIAS will request for verification of identity forward to outside ECP system who has a contract for such verification level

4. The user proves his identity by forwarding his credentials to the component for verification that is located within NIAS system in case of security level 1 or as part of the external ECP system for security level 2 or higher.

5. Proof of verified identity is forwarded to the authorization component of the components service provider. From this point, the process of authentication is completed and begins an authorization procedure whose successful outcome will initiate the service.

6. Authorization component of service provider checks the authority of electronic identity and obtained credentials. Assignment of rights is under the jurisdiction of the body that provides a particular service.

7. The user has consumed/not consumed electronic service.

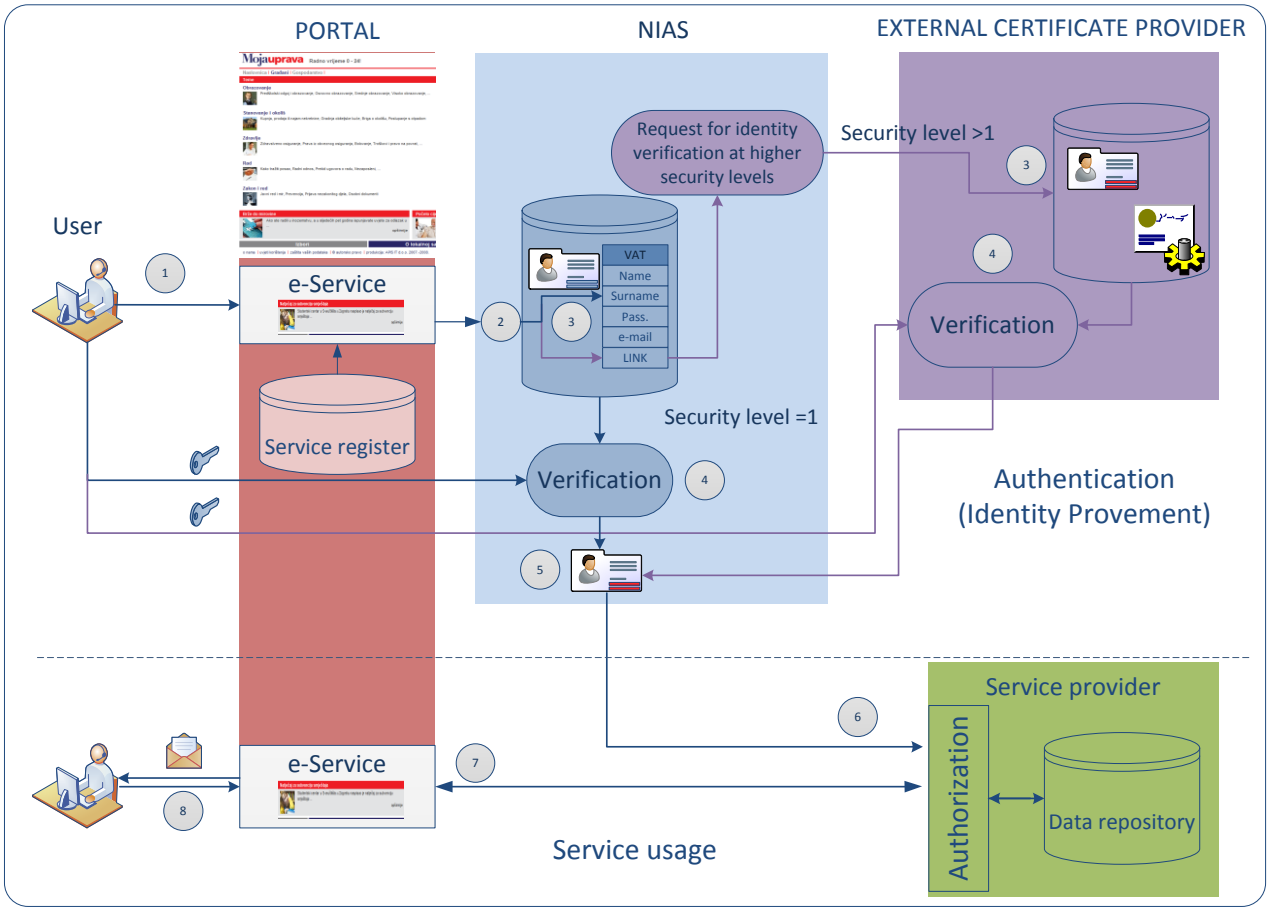

Figure 3. Use of electronic identity in the e-Government

3.1. Principles of assigning the security levels

The security levels are defined as the degree of certainty that the user is correctly identified with their electronic identity. In this context, authentication security levels are defined as a result of fulfilling a number of requirements that ensure two components:

- Satisfying level of confidence in the process of proving the identity in the creation of electronic credentials, which is part of the registration phase.

- Satisfying level of confidence in the process of delivery of electronic credentials, which is part of the electronic authentication phase.

Based on the analysis of risks and their impact on the reliability and security of establishing electronic services, Table 2 shows the general proposition of the reference matrix for determining the required Security Level (SL) of some service.

	Level of Risk				
Appearance	Very high	High	Medium	Low	Negligible
Almost sure	*	*	SL-3	SL-3	SL-3
Very likely	*	SL-4	SL-3	SL-3	SL-2
Moderately	SL-4	SL-4	SL-3	SL-2	SL-1
Unlikely	SL-4	SL-3	SL-2	SL-2	SL-1
Rare	SL-3	SL-3	SL-2	SL-1	SL-1
* Not applicable to a remote user authentication systems					

Table 2. Reference matrix to determine the required safety levels

The lowest security level (SL-0) presents the level at which the access to the service is allowed without the need for authentication or authorization mechanisms. Security level 1 (SL-1) is used to control and facilitate access to services and data with a low level of required protection. The mechanism used for proof of identity at this level the username and password (login/password). Security level 2 (SL-2) can be considered as a medium level of protection. In addition to identification and authentication using a username and password in the authentication procedure must be used at least one mechanism to prove the ownership of a certain object by users who access the service, such as a token that generates one-time passwords OTP.

Security level 3 (SL-3) is designed for services that require a high level of protection. This level is based on public key infrastructure (PKI). The highest security level (SL-4) is intended to access services that require the highest level of protection. In addition to PKI, biometric methods can be used. In addition to these basic divisions, the individual sub-levels can be further developed on the basis of certain technological solutions applied as shown in Table 3.

Security levels		
Level 0 (SL-0)	Level 0.1	Free access without identification
	Level 0.2	Access based on the e-ID
	Level 0.3	Access based on pseudonyms
Level 1 (SL-1)	Level 1.1	Username and password
	Level 1.2	User name and OTP
Level 2 (SL-2)	Level 2.1	Smart card
	Level 2.2	Security token
Level 3 (SL-3)	Level 3.1	Smart cards with PKI support
	Level 3.2	Hardware Security Module (HSM)
Level 4 (SL-4)	Level 4.1	PKI with biometric method (fingerprint)

Table 3. Elaboration of security levels and additional sub-levels

4. Conclusion

Abovementioned model of comparing security levels with the electronic service sophistication level is representing practical implementation of the theoretical model in the public administration in Croatia. Furthermore, implementation is followed with the quantitative analyses of the budget saving as well as the improvement of the citizen-public administration communication since according to the Central Bureau of Statistics (http://www.dzs.hr) a relatively low share of the usage of e-government services (47% in 2017) showed that the usage of e-government services was still not widespread, although it slightly increased (Figure 4). According to same statistics, the real usage of e-government services is in a real sector where most of the enterprises (more than 90%) in different activities (except manufacturing) use electronic services provided by different governmental bodies through NIAS system with full realization of its benefits.

Online government services enable citizens or representative of a business entity to access them at any time and from anywhere, regardless of working time or physical location of individual institutions. However, in such non-secure electronic environments, it is necessary to provide a mechanism that will allow reliable identification of both parties in communication. This is accomplished in a way that each participant is given an appropriate electronic identity in the e-Government, assigned and guaranteed by the reliable component, NIAS, in which both parties (user and service provider) have full confidence.

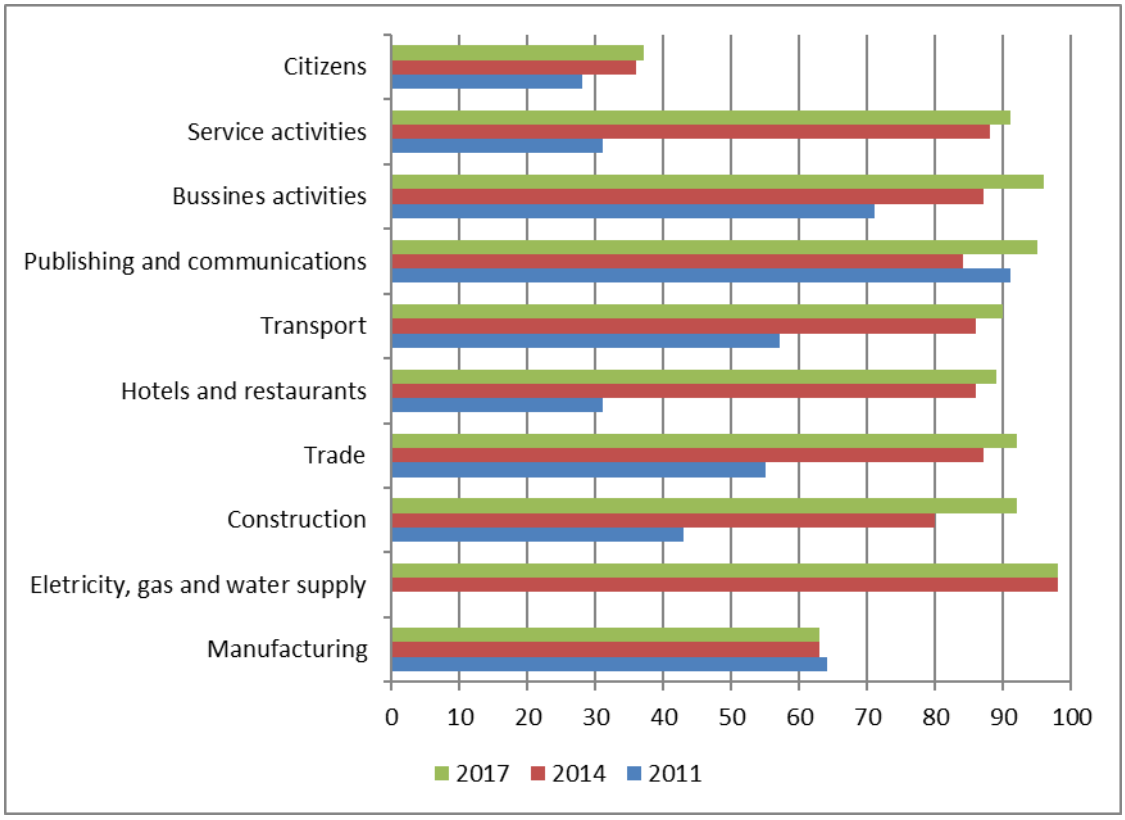

Figure 4. E-government usage (in %) by citizens and in enterprises by activities

5. References

[1] Czech POINT, http://www.czech.cz/en/Life-Work/How-things-work-here/Law/Czech-POINT-%E2%80%93-aid-for-public-administration-in-the (2018-01-29)

[2] Government gateway, http://www.gateway.gov.uk/ (2018-01-29)

[3] Mobile Phone Signature & Citizen Card, https://www.buergerkarte.at/en/ (2018-01-29)

[4] STORK 2.0 project https://www.eid-stork.eu/ (2018-01-29)

[5] Swedish Government Secure Intranet, www.tutus.se/cases/sgsi.html (2018-01-29)

[6] United Nations E-Government Survey 2014, E-Government for the Future We Want, http://www.unpan.org/e-government (2018-01-29)

[7] VANguard, vanguard.business.gov.au (2018-01-29)

[8] X-Road Europe, https://www.x-road.eu/about.html (2018-01-29)