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.

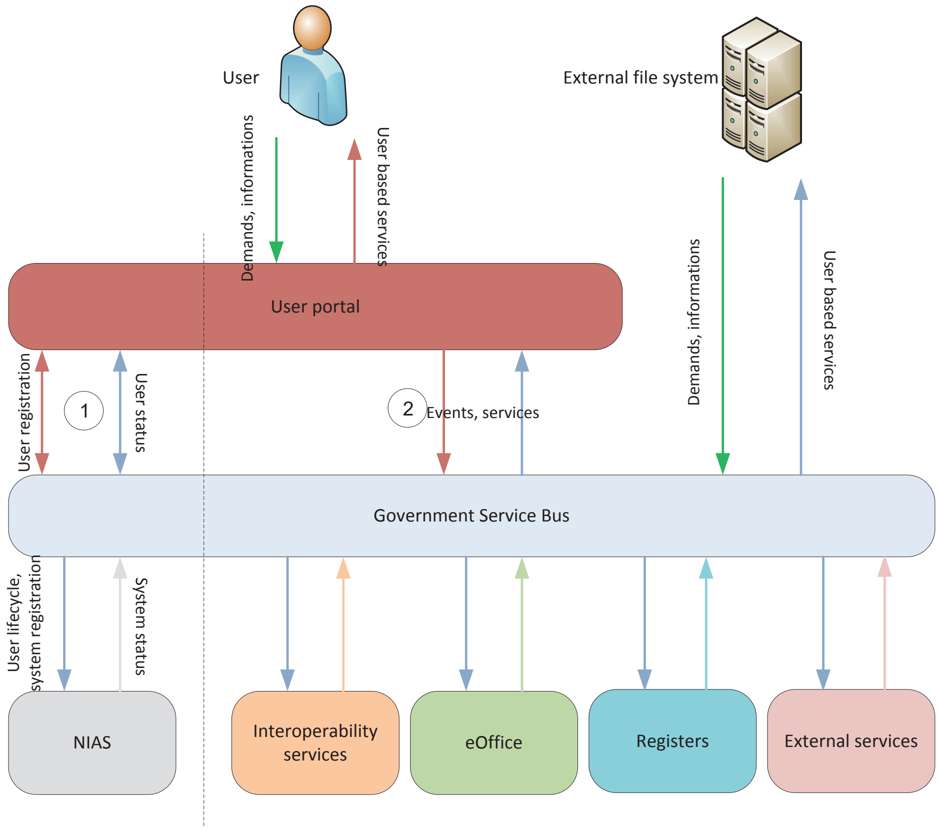

Figure 1. Relationship of NIAS to other building components of Croatian e-Government Initiative

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.

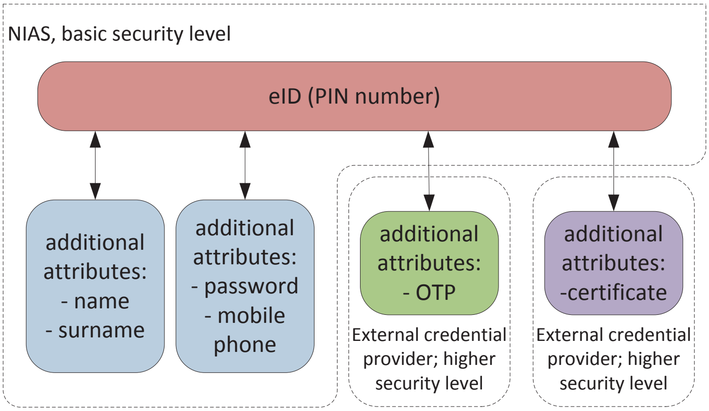
NIAS, basic security level
eID (PIN number)
additional attributes: - name - surname
additional attributes: - password - mobile phone
additional attributes: - OTP
External credential provider; higher security level
additional attributes: -certificate
External credential provider; higher security level

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.

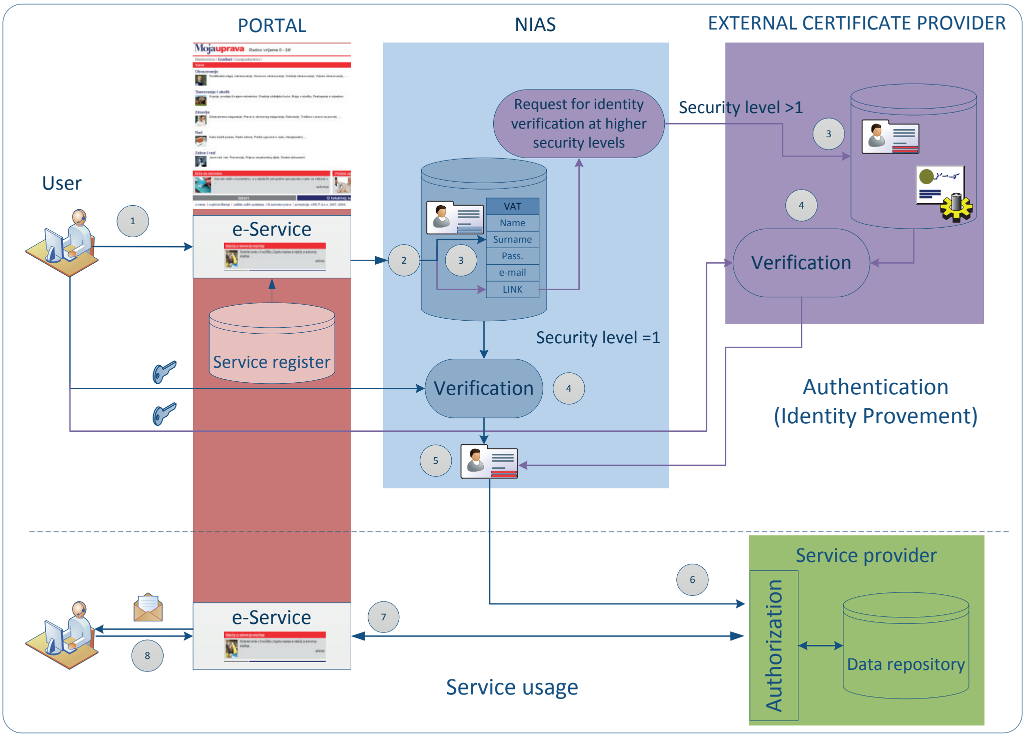

Figure 3. Use of electronic identity in the e-Government

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.

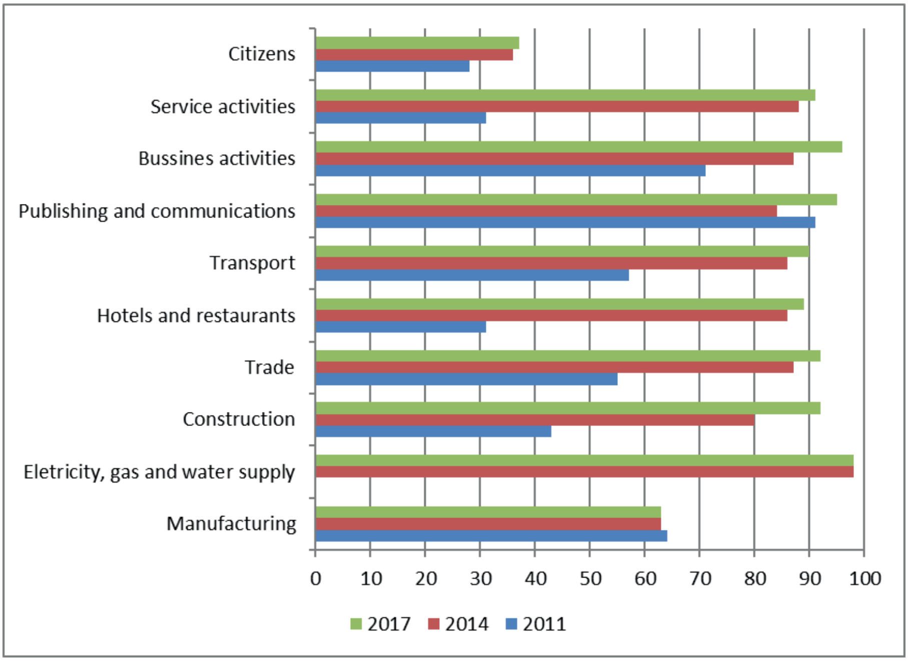

Figure 4. E-government usage (in %) by citizens and in enterprises by activities

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)

DIGITAL MATURITY IN THE ADMINISTRATION OF A UNIVERSITY OF APPLIED SCIENCES

Katrin Hummel[1] and Birgit Schenk[2]

DOI: 10.24989/ocg.v335.25

Abstract

Digital Transformation is very slowly coming within the reach Public Administration in town, city, county, state and the federal government. If and how it reaches Public Administration in the Universities of Applied Sciences (UAS) however, has not yet being analyzed. The UAS point out that they have a strong practical orientation and devote themselves to this in their research. Therefore, they have research programs and lecture programs focusing on Digital Transformation. Coming face to face with this, the question arises whether the Digital Transformation has not just found its way into research and teaching but also into the administration of UAS. This paper describes an analytical model for assessing digital maturity and then addresses this question through an example of a UAS in Baden-Württemberg.

1. Introduction

The UAS in Baden-Württemberg are on the one hand public institutions with bureaucratic administrative structures but on the other hand they are similar to a private business with their given autonomy and competition amongst themselves. [1] Their concern is to provide society and the economy with the strength for innovation through an up-to-date combination of science and practical orientation as well as excellent quality teaching. [2] In addition to their core responsibility for research and teaching they are also responsible for further adult education as knowledge for life-long learning. Countless papers as well as new teaching materials and methods prove that they achieve their responsibilities by working on Digital Transformation. The UAS administration has the responsibility to unburden and support the areas of research, teaching and further education and thus becomes a service provider. Because of this the UAS administration is different from other public administration. Considering digitalization this means that its transformation should be stretched to the areas of research, teaching, further education and administration.

The government of Baden-Württemberg stresses the importance of digitalization in its strategy with their statement: “We will support the Universities of Baden-Württemberg for further development of their business processes concerning research, teaching and knowledge transfer to make use of the possibilities offered by digitalization.”[3] and the Commission of Research and Innovation (EFI) explains in its report that digitalization is the major requirement for excellence in research and teaching [3].

[1] HVF Ludwigsburg, University of Applied Sciences, Reuteallee 36, 71634 Ludwigsburg

[2] HVF Ludwigsburg, University of Applied Sciences, Reuteallee 36, 71634 Ludwigsburg, Birgit.Schenk@hs-ludwigsburg.de

[3] *„Wir werden die baden-württembergischen Hochschulen dabei unterstützen, ihre Geschäftsprozesse weiterzuentwickeln, um die Möglichkeiten der Digitalisierung zu nutzen: in der Forschung, in der Lehre und beim Wissenstransfers.“*[3]

The expectations of the service ability of UAS are rising [4] but not to the same extent as the means available. To bridge the gap between the demands and resources [5] there must be an increase in efficiency in all aspects to achieve a better provision of service and higher economic efficiency. [6] This could be achieved by using digital technology as shown by the following examples. Since the Eighties students at the University of Vienna have been able to obtain information or to enroll by using a screen text. [7] In Hungary the campus management system NEPTUN [8] is in use as are similar systems in Germany e.g. Fernuniversität Hagen [9]. So the question arises: if the Digital Transformation of UAS administration already exists and up to what extent Digital Maturity has been reached.

In order to analyze the extent of the digitalization and assess the maturity level of UAS administration, we need a general maturity model and information about their core processes to be able to design a data gathering instrument based on the maturity model and tailored to UAS as a vision of a "mature" UAS administration. Additionally we need a vision of a "mature" UAS administration to be able to define the scale for measuring the degree of maturity.

2. Degrees of Maturity and Maturity Models

First of all the core processes were identified within a framework of an organizational analysis and illustrated in a process map. Since there is no digital maturity model in the literature suitable for every organization and nothing specifically for UAS administration, the development of a digital maturity model followed. 12 different digital maturity models were identified and compared (see table 1). All of them were developed through business consultants, scientists, researchers and all of them are being successfully used in different organizations such as companies and ministries.

Each maturity model consists of (a) dimensions to define the business areas and (b) the indicators to check the extent of digitalization within the dimensions, (c) maturity levels for the assessment of the degree of digitalization. Comparing the models we noticed that the core dimensions are similar even if they are split in different ways. So we needed to define the number of maturity levels, to identify the relevant dimensions and to decide upon the indicators for the measurement. Considering the given circumstances of core processes and structures of UAS we worked through these three steps (a) to (c) identifying nine dimensions, each having equal importance, and their indicators (see table 1) as well as five maturity levels beginning with 0 (no digitalization up to minimal digital implementation) up to 4 (complete digitalization).

A questionnaire was designed based on the newly developed maturity model. To guarantee that the participants understood each dimension and its indicators additional explanations were given. The field survey took place in a faculty of one of the biggest UAS in Baden-Württemberg. The faculty was chosen as a random sample. 60 people were invited to complete the questionnaire online. 34 were professors, six scientists and six lecturers – representing the lecturing and research perspective dependent on the administration, eleven administrative employees and one secretary, one IT-administrator, one head of marketing – all representing the administration.

Maturity Model of Dimensions	Universität St. Gallen [10]	Deloitte [11]	Hochschule Ulm [12]	Wolf/Stroschen [13]	Bundesministerium des Innern [14]	BSP Business School Berlin [15]	FOSTEC & Company [16]	Appelfelder/Feldmann [17]	Netode AG [18]	DRP Reifegrad Fraunhofer [19]	Forrester [20]	Accenture [21]	SUM
Organizational structure	1	1	1	1	1		1		1		1	1	9
Information- and Communication Technology	1	1		1	1	1	1	1	1		1		9
Business Processes	1	1	1	1	1			1	1			1	8
Customer Experience / Customers Perspective	1	1	1		1	1	1	1	1				8
Culture & Expertise	1	1		1	1	1			1	1	1		8
Strategy	1	1			1	1	1		1	1		1	8
Employees			1	1	1	1		1		1			6
Products & Services	1		1	1				1	1				5
Collaboration	1			1					1	1			4
Production / Delivery			1	1				1					3
Business Models			1					1					2
Networking with Partners				1				1					2
Supplier & Partners			1					1					2
Agile Methods			1							1			2
Services			1									1	2
Data Management				1				1					2
Controlling / Continuous Improvement Proc.					1						1		2
Transformation Management	1												1
Communication				1									1
Production 4.0									1				1
Methods & Tools					1								1
Leadership						1							1
Competition							1						1
Value-added Chain				1									1
Standardization					1								1
Number of Maturity Levels	5	-	5	5	5	4	10	5	5	5	4	5	5,3

Table 1. Dimensions of the identified 12 maturity models

3. A "Vision" of a digitalized UAS

As already explained five grades of digitalization beginning with 0 (no digitalization up to minimal digital implementation) up to 4 (complete digitalization) were defined. So the question arises, what is meant by the highest score "complete digitalization"? One would think that it primarily aims at controlling the flow of processes by means of "digital technologies" – i.e. IT systems. That is only one part of the vision limited to an e-Government-perspective [22] which focuses more or less on the core processes of a UAS. Considering the whole organization, the research results of Digital Transformation [23] and working through all dimensions of the different maturity models, the vision is a broader one. Our vision of a digitalized UAS is an organization which makes use of digital technologies to benefit in every aspect such as offering new and additional (e-)services to their customers as well as supporting and empowering their employees to do their work in an up-to date way. Its goal is to speed up workflow processes, to give the employees more time to focus on important work and to provide them with the opportunity to be agile in order to meet new expectations, new requirements and new trends, to be able to act and to adapt to changing circumstances in order to fulfil their task in providing society and the economy with the strength for innovation through an up-to-date combination of science and practical orientation as well as excellent quality teaching and the transfer of knowledge.

To achieve this goal, each of the chosen dimensions is needed. For example digitalization needs cultural change. Several digital transformation projects are proof that digitalization focusing only on digital technologies does not meet the expected results as long as there is no digital culture. Analogue procedures are reproduced accurately in digital procedures, but a worse analogue procedure is a worse digital procedure. Behaviour patterns and ways of thinking, the people's mindset and their mental horizons need to be changed so that they "think and act" in a digital way. Only then can the benefits of digital transformation be derived. [11] This means i.e. that employees need digital abilities and recruiting employees need to consider this ability by selection processes. Additionally employees need to enhance their digital and non-digital competencies through an extensive education program to stay up-to date and to continually develop their abilities. [14,15,16,19]

4. Results and Discussion

Thirty-eight people took part in the questionnaire. This represents 63.3 percent of the sample. The whole of the results are shown in table 2. For the assessment we used the marking where each indicator was positioned on the scale from 0 to 4. The abbreviation "RG" stands for the average of each indicator as well as for its maturity level, ∅ shows the maturity level of the dimension.

Dimension	Indicator	RG	∅
Organizational structure	There is one person in charge of the digitalization of the administration	1,4	1,3
	Cross-departmental and cross-functional teams work on and drive the projects of digitalization.	1,3	
	The UAS provides personnel and financial resources for the digitalization of the administration.	1,7	
	The administration has the ability to react /to adapt to digital changes and its requirements.	0,8	
Information- and Communication Technology	ICT meets the expectations and needs of students, researchers, lecturers and employees.	1,7	1,3
	The IT-department offers and uses up-to date technology and is able to develop and implement it in short-term.	1,2	
	All IT-systems are connected and they exchange data in the sense of "once only"	1,1	
	There is a central data storage for customer data which can be used by all departments who need it.	1,3	
	Electronic file management is implemented throughout the whole organization.	0,7	
	IT-Infrastructure offers new possibilities and supports collaboration.	1,8	
Business Processes	Standardized processes are automated.	1,3	1,1
	Continuous improvement of digitalization and standardization is implemented.	1,1	
	Digitalized business processes - without any changes of media usage.	1,1	
	The business processes will be continuously improved.	1,4	
	The business processes are transparent and easy to understand.	0,9	
	The business processes are measured via key performance indicators.	1	
Customer Experience / Customer Perspectives	All communicational channels (e.g. email, sms, paper, face to face …) are available for the customers to address their issues.	1,4	1,0

(students, lecturers, researchers, employees)	Information is tailored to the customers' needs.	1,2	
	User behavior is tracked and used to improve processes and services.	0,7	
	Feedback of customers is valued and analyzed to improve services and processes.	1,1	
	Customers are able to track the processing of their issues.	1,0	
	Customers are involved in process design and service development	0,9	
	New trends and technologies are used for communicating with customers.	0,9	
Culture	The administration knows that digitalization is a success factor for competition.	1,5	1,1
	The administration is ready for digital change and has the ability to drive digital change.	0,7	
	The administration has a culture of constructive criticism. Its zero-defect culture promotes dealing with errors actively and openly in order to benefit from potential improvements.	1,0	
	The UAS management encourages and promotes digital innovation in administration.	1,4	
	The management are prepared to take risks into account when it comes to digital innovation in existing business of the UAS.	0,9	
Service Delivery	Up-to date technology (e.g. customer relationship management systems) supports service delivery completely.	1,0	1,0
	All services offered by the administration are digitalized from customer back to customer.	0,9	
	Value added e-services are all well-known and transparent.	0,9	
	Customer feedback management is implemented.	1,0	
Strategy	The UAS has a vision of digitalized administration.	0,9	0,9
	A holistic and integrated strategy for digitalization of administration exists and is embedded in the Structural and Development Plan of the UAS.	1,1	
	All employees participate in the strategy development.	1,1	
	All employees know the digital strategy of administration.	0,6	
	The management of administration gives a good example when it comes to digitalization and they work on it.	0,9	
	All goals of the digital transformation are „SMART“ (specific, measurable, achievable, realistic, timed).	0,7	
	All actions to digitalize administration follow a concerted policy.	0,7	
	The strategy of Digital Transformation is regularly checked and adapted to new trends and technology.	1,0	
Collaboration	Mobile devices support cross-departmental and cross-functional collaboration.	2,5	2,1
	All employees have the choice to work mobile.	2,4	
	Teams optimize their collaboration through mobile work.	2,1	
	The administration is connected and uses collaboration platforms.	1,8	
	New Work-methods and techniques are used to improve collaboration.	1,6	
Employees	The administration considers the digital ability of applicants in their recruiting procedures and selection processes.	1,5	1,4
	The administration offers an extensive education program focusing on digital competencies of their employees.	1,0	
	Employees are motivated, asked and urged to extend their digital ability.	1,4	
	The administration has a strategic HR development program to improve the digital ability of employees.	0,9	
	All employees actively use their digital ability, methods and techniques.	1,7	
	All employees express a strong interest in participation in the digital transformation of their UAS.	1,9	
	All employees of the administration use agile methods e.g. Scrum, Design Thinking, etc.	1,1	
Digital Maturity Level of the UAS administration			**1,2**

Table 2. Maturity levels of dimensions and its indicators

The results of the analysis show that the digital maturity level for the UAS administration is generally low with an average of 1.2. Figure 1 gives an idea of the overall status. The diagram makes it clear with the exception of the dimension “*Cooperation*” that all dimensions stand at level 1. Level 1 is defined as “It is recognized that digital transformation management is necessary” which means that although it has been recognized no concrete steps have been taken. It is worth noting that the dimension “cooperation” comes out above average with the digital maturity level of 2.1 compared with the other dimensions. It is also worth noting that the dimension “strategy” comes out with the worst average of 0.9 compared with the others. This is all the more remarkable since at strategic thought and action is taught at the UAS.

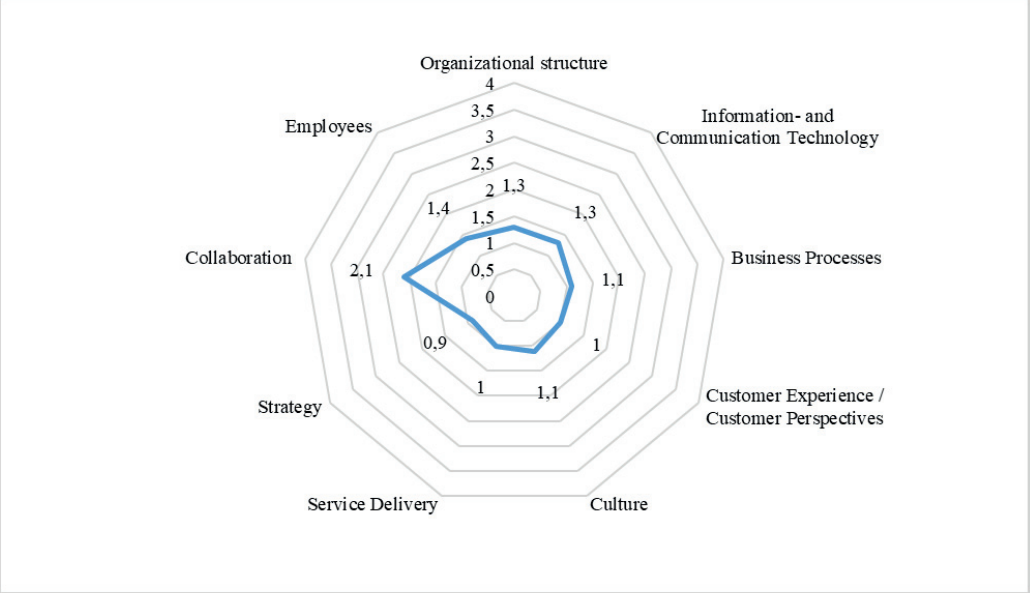

Figure 1. The Digital Maturity Level of the UAS [24]

The participants were particularly critical that the UAS is not able to react quickly to changing demands. This can be seen from the indicators "preparedness to be mobile" and "ability to change" as well as "ability to take a risk". Above all the participants criticized the performance of the core processes, the lack of participation of clients while designing the business processes and the missing e-document management / e-archive. The possibility of mobile work which supports internal collaboration received a positively response. Additionally the participants commented that they would like to be involved in the process and implementation of Digital Transformation.

Looking at the results the question arises why digitalization caused profound changes only in the private sector and didn't reach the administration of a UAS. This is all the more remarkable when we consider the fact that the UAS focuses on the subjects Economy, IT and Technique and therefore cooperates with the private sector to successfully fulfill its core responsibilities. Maybe the strength of their practical orientation of the UAS is limited to theoretical work in research and teaching. Maybe there is a border in transferring research findings and knowledge to the internal organization. When we searched for the digitalization strategies of the UAS, we could only find two UAS which had their strategy online and wrote about it.

Another explanation may offer the implementation of the digital strategy for Baden-Württemberg. Even if *strategy* emphasizes that business processes may be supported, the implementation focuses on research and teaching e.g. they started a new program for "e-Learning" which supports new teaching methods and materials and they initiated a network called "Hochschulnetzwerk Digitalisierung der Lehre in Baden-Württemberg". [25] There are no action plans or activities focusing on campus management systems and the business processes connected to research and teaching.

The administration of UAS is hierarchically and traditionally organized like most of the public administration. Therefore they show little willingness to change anything, if the change is not driven by the management. The management drives change if they have to face competition or to meet financial deficits or to attract new employees in the time of demographic change. The pressure of change is not yet high enough. This is proved by their hesitant attitude to implement new software and drive digital transformation overall [26].

5. Summary

This paper addressed the question whether the Digital Transformation has only found its way into teaching and research as a topic but not into the administration of UAS. Considering the results of the study the question can be answered with “no”. The digital maturity of the chosen University of Applied Sciences is 1.2 on a scale ranging from 0 to 4. The lowest score of the nine analyzed dimensions (organizational structure, information and communication technology, business processes, customer experiences and perspectives, culture, service delivery, strategy, collaboration and employees) could be found in *strategy* with 0.9. This is surprising because each University of Applied Sciences has to publish annually a so-called “Structural and Development Plan” which is examined by the Ministry of Education, Science and Culture of Baden-Württemberg.

Based on the hypothesis that the chosen UAS represents all UAS in Baden-Württemberg alarm bells should be ringing in times of Digital Transformation. The results show that the UAS administration is not aware of the importance of digital change, nor willing, and therefore not prepared to drive the digital change. Following the statement of Prof. Scheer [27] who said: “Only if the administration is innovative, the areas of teaching and research are able to proceed in the digital future.” this underlines the necessity to drive the Digital Transformation in all areas of a UAS: research, teaching, further education *and* administration.

The study was limited to one faculty of one of the biggest UAS in Baden-Württemberg. So the conclusions of the results are limited and can only be seen as an indication. Additionally the majority of participants represented the customer perspective, not the perspective of administration. Therefore, to verify the findings, further research is necessary with a bigger sample.

6. References

[1] See KLEIMANN 2009, p. 7f. https://hishe.de/fileadmin/user_upload/Veranstaltungen_Vortraege/2009/Forum_Pruefungsverwaltung_2009/03_HISForumPV_09_Kleimann.pdf, 03.11.2018

[2] See NICKEL 2009, p. 66.

[3] EXPERTENKOMMISSION FORSCHUNG UND INNOVATION 2016, S.29 https://www.e-fi.de/fileadmin/Gutachten_2016/EFI_Gutachten_2016.pdf, Stand:16.06.2018.

[4] TEUSCHER 2016, Entwicklungsperspektiven von Hochschulen für Angewandte Wissenschaften – Chancen und Risiken. Strategische Entwicklung von Hochschulen.

[5] ZECHLIN 2007, p. 115.

[6] SCHEER 2015, p.2 https://www.gategermany.de/fileadmin/dokumente/angebote/Kongresse/Marketing-Kongress/2015/Web_Scheer_Whitepaper_Nr__8_Hochschule_4_0.pdf, 31.08.2018.

[7] MUPID https://link.springer.com/chapter/10.1007%2F978-3-642-82946-8_1 3.2.2019

[8] NEPTUN in Ungarn, siehe http://sziu.hu/neptun oder https://en.uni-nke.hu/document/en-uni-nke-hu/neptun-user_s-guide.original.pdf 3.2.2019

[9] FERNUNI HAGEN, https://www.fernstudium-wiwi.de/fernuni-hagen-einschreibung-und-rueckmeldung/ 2.2.2019

[10] BACK/BERGHAUS 2016, S.8 https://aback.iwi.unisg.ch/fileadmin/projects/aback/web/pdf/digitalmaturitymodel_download_v2.0.pdf, 22.10.2018.

[11] DELOITTE 2018, S.10 https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/deloitte-digital-maturity-model.pdf , 22.10.2018.

[12] PLECHATY/LANG 2017 http://reifegradanalyse.hs-neu-ulm.de/questions.php#firstPage, 22.10.2018.

[13] WOLF/STROHSCHEN 2018, p. 63.

[14] BUNDESMINISTERIUM DES INNERN 2011, p.10 https://www.verwaltung-innovativ.de/SharedDocs/Publikationen/Regierungsprogramm/reifegradanalyse_prozessmanagement.pdf?__blob=publicationFile&v=1, 22.10.2018.

[15] BSP Business School Berlin GmbH 2016, p. 6ff. https://kommunikation-mittelstand.digital/content/uploads/2017/01/Leitfaden_Ermittlung-digitaler-Reifegrad.pdf, 22.10.2018.

[16] FOST o.J. https://www.fostec.com/de/kompetenzen/digitalisierungsstrategie/digital-readiness/, 22.10.2018.

[17] APPELFELLER/FELDMANN 2018, p. 4.

[18] FISCHER 2017, p. 21 https://www.netnode.ch/blog/was-niemand-ueber-design-thinking-sagt, 22.10.2018.

[19] FRAUNHOFER BIG DATA https://www.bigdata.fraunhofer.de/content/dam/bigdata/de/documents/Publikationen/DRP_Reifegrad_Schnellcheck_FhBigDataAllianz.pdf, 22.10.2018.

[20] GILL, M./VAN BOSKIRK 2016, p. 3 https://forrester.nitro-digital.com/pdf/Forrester-s%20Digital%20Maturity%20Model%204.0.pdf, 22.10.2018.

[21] HINKEL/PFANNES 2016, p. 4 https://www.accenture.com/t00010101T000000__w__/de-de/_acnmedia/PDF-36/Accenture-Digitalisierungsindex-OV-05-2016-(003).pdf, 10.08.2018.

[22] ALMUFTAH, H., WEERAKKODY, V., SIVARAJAH U., Comparing and Contrasting e-Government Maturity Models: A Qualitative-Meta Synthesis, 2016. In: Scholl et al. Electronic Government and Electronic Participation. doi:10.3233/978-1-61499-670-5-69, 8.2.2019.

[23] GONÇALVES DOS REIS, J. C., MELAO, N., AMORIM, M., Digital Transformation: A literature Review and Guidelines for Future Research. 2019, DOI: 10.1007/978-3-319-77703-0_41

[24] HUMMEL, K. 2019, p. 70

[25] MINISTERIUM FÜR INNERES, DIGITALISIERUNG UND MIGRATION BADEN-WÜRTTEMBERG 2017, p. 70 https://www.digital-bw.de/impressum?redirect=%2Fweb%2Fguest%2Fdigitalisierungsstrategie%3Fredirect%3D%252F, 21.06.2018.

[26] GLICH et al. 2017, p. 2f. www.gfhf.net/wp-content/uploads/2016/07/0083_Jungermann-Digitalisierung-der-Verwaltung.pdf, 31.08.2018.

[27] SCHEER 2015, p. 28 https://www.gate-germany.de/fileadmin/dokumente/angebote/Kongresse/Marketing-Kongress/2015/Web_Scheer_Whitepaper_Nr__8_Hochschule_4_0.pdf, 31.08.2018.