


Chapter 16

Cybersecurity and Electronic Services Oriented to E-Government in Europe

Teresa Magal-Royo

 <https://orcid.org/0000-0002-7640-6264>
Universitat Politècnica de Valencia, Spain

José Macário de Siqueira Rocha

Leading Management Technology, Spain

Cristina Santandreu Mascarell

Universitat Politècnica de Valencia, Spain

Rebeca Díez Somavilla

Universitat Politècnica de Valencia, Spain

Jose Luis Giménez López

Universitat Politècnica de Valencia, Spain

ABSTRACT

Cybersecurity in Europe as the rest of the world has been legislated for only 20 years. Numerous governmental institutions such as councils offer electronic services through their recently created electronic offices. In all of them, the volume of citizens who register temporarily or permanently to request online services related to the processing of documents and services with the government has increased significantly since the pandemic. Confinement has forced users to request numerous online services where authentication is one of the most relevant aspects to access safely and securely. European Union through the Connecting Europe Mechanism, CEF projects of the European Health Executive Agency, and Digital HaDEA has allowed numerous institutions to connect through the eIDAS created to establish trust in electronic transactions between individuals, organizations, and government entities across European member states.

DOI: 10.4018/978-1-7998-6975-7.ch016

INTRODUCTION

This chapter shows the importance of digital services for public services around the world and in particular to Europe. The European Union has been working on the regulation and control of secure digital transactions in Europe for more than 20 years and it will mention the existing regulations including the concepts Electronic identification (eID) and Electronic IDentification, Authentication and trust Services (eIDAS) used by both companies as public institutions.

Due to confinement, the increase in electronic services in public electronic offices worldwide has increased enormously and therefore it is necessary to pose new challenges in the control and management of sensitive data of citizens who access and share their data with administrations public.

On the other hand, the problems related to cyberattacks are very similar to those that we can find in private companies, therefore, the most important challenge for Europe will be, on the one hand, the detection of the types of massive attacks that can affect the use of data of citizens of the electronic headquarters and on the other the containment plans that are needed to control it at European level

Finally, we will mention examples of CEF projects that promote the implementation and use of the mechanisms offered by the European Union in the eIDAS regulation in electronic public services throughout Europe.

As cybersecurity remains a challenge for government websites: Only 20% of all URLs assessed meet half of the 14 basic security criteria evaluated. This underlines the importance of significantly enhancing website security levels to ensure that users can trust public sector websites and services. (EC, 2020)

In fact, e-Government refers to the use by national or local governmental authorities of ICTs that can reshape the relations with citizens and businesses. It contributes to the evolution of smart cities when ICTs are integrated in strategies for citizen participation to public services and policy, (Webster & Leleux, 2018).

The report e-Government Benchmark 2020 created by European Commission, shows remarkable improvements across the board. More than three out of four public services can be fully completed online (78%). Users can find the services they are looking for via portal websites 95% of the time, and information about these services online nearly 98% of the time. European countries should improve the implementation of digital enablers in eGovernment service delivery. Users use their own national eID for only half (57%) of the services that require online identification. Moreover, only half (54%) of online forms contain pre-filled data to ease completion. Users who want to obtain a service from another European country can do so in 62% of the services for citizens and 76% of the services for businesses. Citizens can use their own national eID solution for only 9% of the services from other countries. For businesses this number jumps to 36%. The cross-border use of digital public services are problems with access to procedures requiring authentication. Foreign national eIDs are accepted for only 9% of the services that citizens can access with a domestic eID. This indicates that the cross-border acceptance of eIDs still requires more research and implementation in national or local governmental institutions.

e- Government as a Challenge in Europe

Governments are institutions that contribute to governance a country or a region. Representative governments seek and receive citizen support, but they also need the active cooperation of their public servants (Carter & Belanger, 2005). E-governance, meaning electronic governance, has evolved as an information-age model of governance that seeks to realise processes and structures for harnessing the potentialities

19 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/cybersecurity-and-electronic-services-oriented-to-e-government-in-europe/284158

Related Content

Forensic Investigation-Based Framework for SDN Using Blockchain

Sonam Bhardwaj, Rochak Swamiand Mayank Dave (2021). *Revolutionary Applications of Blockchain-Enabled Privacy and Access Control* (pp. 74-98).

www.irma-international.org/chapter/forensic-investigation-based-framework-for-sdn-using-blockchain/274699

Balanced Scheduling Method of Network Information Resources for Cloud Storage

Xiang Maand Zhan Li (2022). *International Journal of Information Security and Privacy* (pp. 1-17).

www.irma-international.org/article/balanced-scheduling-method-of-network-information-resources-for-cloud-storage/310514

An Effective and Computationally Efficient Approach for Anonymizing Large-Scale Physical Activity Data: Multi-Level Clustering-Based Anonymization

Pooja Parameshwarappa, Zhiyuan Chenand Gunes Koru (2020). *International Journal of Information Security and Privacy* (pp. 72-94).

www.irma-international.org/article/an-effective-and-computationally-efficient-approach-for-anonymizing-large-scale-physical-activity-data/256569

Identity Management for Wireless Service Access

Mohammad M.R. Chowdhuryand Josef Noll (2008). *Handbook of Research on Wireless Security* (pp. 104-114).

www.irma-international.org/chapter/identity-management-wireless-service-access/22043

The Dark Society: Two Decades Later – Ulrich Beck and His Publication Risk Society Towards a New Modernity

Maximiliano Emanuel Korstanje (2020). *International Journal of Risk and Contingency Management* (pp. 57-67).

www.irma-international.org/article/the-dark-society/252182