Chapter 2
Cybersecurity in Europe: Digital Identification, Authentication, and Trust Services

Joni A. Amorim
https://orcid.org/0000-0002-9837-9519
Universidade Estadual de Campinas (UNICAMP), Brazil

Jose-Macario de Siqueira Rocha
Universitat de València, Spain

Teresa Magal-Royo
https://orcid.org/0000-0002-7640-6264
Universitat Politécnica de València (UPV), Spain

ABSTRACT

Information security is increasingly necessary between citizens and public services. In a nearby environment, such as cities, there are digital services and infrastructures that help improve our quality of life. Secure access to services must be regulated and offer trust to the user. Initiatives like the Regulation from European Union, (EU) N° 910/2014 of the European Parliament and the Council intend to favour solutions for problems like interoperability and cybersecurity. In this chapter, two European countries are considered so that implementations of the electronic identification, authentication, and trust services are presented and discussed. The main contribution is a description of relevant European projects, a first step necessary to propel further research on this topic. The chapter also presents the current challenges for the consolidation of the technology used and for the adaptation of the electronic services offered by public administration bodies to citizens.

DOI: 10.4018/978-1-7998-6975-7.ch002

INTRODUCTION

According to the Netherlands Environmental Assessment Agency, PBL (2016), the European Union has more than 800 cities with more than 50,000 inhabitants. Europe is considered to be highly urbanized, with different types of regions: monocentric, dispersed, linear and polycentric urban regions. These many regions in Europe are now undergoing a digital transformation since cities are starting to use smart technologies. Smart Cities represent the future of urban development in a world where daily activities depend more and more on different kinds of technologies like the Internet of Things, (IoT) and Artificial Intelligence, (AI). A more interconnected world demands improved electronic services that enable interactions between businesses, citizens and public authorities. The increased interconnection suggests new cyber risks in connection with technologies like IoT (Kalkan & Rasmussen, 2020), AI (Hintze, 2016). Pedersen & Tjørnehøj suggest: *"…e-government lacks theoretical models that can increase our understanding of the relationship between the external environment and e-government investments and how these investments pay off by renewing public sector* capabilities", (Pedersen & Tjørnehøj, 2018).

Authors also advocate that the reduction of operating costs together with a high level of integration of processes are essential if the intent is to provide efficient services for citizens. Pedersen & Tjørnehøj listed five main characteristics of transformational governments as being (i) citizen centricity, (ii) single points of contact, (iii) flexible service delivery, (iv) integration, and (v) reengineering and optimization. All this process needs a progressive digital transformation of the society including citizens. According to Vial, this transition may be understood as: *"…a process where digital technologies create disruptions triggering strategic responses from organizations that seek to alter their value creation paths while managing the structural changes and organizational barriers that affect the positive and negative outcomes of this process" (Vial, 2019).*

The inherent complexity associated to definitions like this one suggests different research agendas that may be easily related to cybersecurity, privacy, trust, cyberresilience, etc…

Seppänen et al. (2018), the failure to manage digital services architecture in a city *"…leads into problems in interoperability and holistic development that are the requirements for a fluid digital transformation of governments".* In this way, it is essential to determine the components of the government organization to understand their synergy so that their actions would be aligned to the objectives of each specific organization. On the other hand, it is also essential to consider how organizations would interact with each other and with stakeholders as well while taking into consideration factors like cyber security and privacy.

This context suggests electronic identification (eID) and electronic trust services (eTS) as being enablers of interactions between businesses, citizens and public authorities as suggested by recent regulations from the European Union. The Regulation 910 from the European Parliament and the Council (EPC, 2014). National electronic identification schemes should be interoperable while following a framework consisting of characteristics like common operational security standards, rules of procedure and a reference to a minimum set of person identification data uniquely representing a natural or legal person. This same regulation also implies that cooperation between the states members should involve information exchange experience and good practices.

Since 2000, electronic services managed by the public institutions of the Member States of the European Union are adapting to the new society times in terms of creating cross-border and efficient digital services for their citizens (Al-Hujran et al., 2015). Due to a large amount of digital information and electronic transactions that are currently managed within the context of Smart Cities, the identification