SPRINGER BRIEFS IN CYBERSECURITY

Norberto Nuno Gomes de Andrade
Lisha Chen-Wilson
David Argles
Gary Wills
Michele Schiano di Zenise

Electronic Identity

Springer

SpringerBriefs in Cybersecurity

For further volumes:
http://www.springer.com/series/10634

Cybersecurity is a difficult and complex field. The technical, political and legal questions surrounding it are complicated, often stretching a spectrum of diverse technologies, varying legal bodies, different political ideas and responsibilities. Cybersecurity is intrinsically interdisciplinary, and most activities in one field immediately affect the others. Technologies and techniques, strategies and tactics, motives and ideologies, rules and laws, institutions and industries, power and money—all of these topics have a role to play in cybersecurity, and all of these are tightly interwoven.

The SpringerBriefs in Cybersecurity series is comprised of two types of briefs: topic- and country-specific briefs. Topic-specific briefs strive to provide a comprehensive coverage of the whole range of topics surrounding cybersecurity, combining whenever possible legal, ethical, social, political and technical issues. Authors with diverse backgrounds explain their motivation, their mindset, and their approach to the topic, to illuminate its theoretical foundations, the practical nuts and bolts and its past, present and future. Country-specific briefs cover national perceptions and strategies, with officials and national authorities explaining the background, the leading thoughts and interests behind the official statements, to foster a more informed international dialogue.

Norberto Nuno Gomes de Andrade
Lisha Chen-Wilson · David Argles
Gary Wills · Michele Schiano di Zenise

Electronic Identity

Springer

Norberto Nuno Gomes de Andrade
European Commission, Joint Research Centre (JRC), Institute for Prospective Technological Studies (IPTS)
Seville
Spain

Lisha Chen-Wilson
David Argles
Gary Wills
Department of Electronics and Computer Science
University of Southampton
Southampton
UK

Michele Schiano di Zenise
R&D Division
Positech
Procida
Italy

ISSN 2193-973X
ISBN 978-1-4471-6448-7
DOI 10.1007/978-1-4471-6449-4
Springer London Heidelberg New York Dordrecht

ISSN 2193-9748 (electronic)
ISBN 978-1-4471-6449-4 (eBook)

Library of Congress Control Number: 2014937691

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Foreword

Electronic identities (eIDs) are of vital importance to citizens, governments, and businesses. eID is a core enabler of personal, business, and government processes. The use of eIDs enables a more efficient access to public service and creates trust over the Internet for transaction services.

"Electronic Identity" is a means for people to prove electronically that they are who they say they are and thus gain access to services.[1] The deployment of e-identity will enable governments to offer better government services and reduce administrative burdens. Businesses and consumers use eIDs to enhance business productivity and improve commercial services, such as online bank transactions, signing contracts and procurement, among others.

E-identity is considered as an enabler of the digital economy. The European Union has recognized its importance in invigorating the economy. In its Europe 2020 Strategy, the European Commission drew attention to "the fragmentation that currently blocks the flow of online content and access for consumers and companies"[2] within the envisaged digital single market, and emphasized the need to overcome it. The ultimate aim is to facilitate e-commerce. However, there is still no legal framework for a pan-European system for electronic authentication. The EU aims to overcome the patchwork of different laws, rules, standards, and practices, and to change the legal framework to cross-border transactions. However, it faces national opposition in many member states.

This book is written from a legal and technical perspective.

The legal aspects of electronic identity written by Norberto Andrade examine the core legal and regulatory issues regarding electronic identity (eID) in the European Union. It looks at the main and common objective behind the eID regulatory initiatives and projects developed in the EU: the creation of a pan-European eID legal framework. It elaborates on the obstacles that are hindering the establishment of such scheme and proposes a conceptual framework of principles that could form the basis of a future EU legal framework for the protection and management of digital identities.

---

[1] http://ec.europa.eu/information_society/activities/ict_psp/documents/eid_introduction.pdf

[2] Commission, "Europe 2020: A Strategy for Smart, Sustainable and Inclusive Growth," 19.

Dr. Norberto Nuno Gomes de Andrade, formerly scientific officer at the Information Society Unit of the Institute for Prospective Technological Studies (IPTS), Joint Research Centre (JRC)—European Commission, provides a compelling insight and analysis that are necessary for a broad understanding of the complexities that lurk in the eID regulatory initiatives. This book is stimulating and informative and Dr. Andrade has ensured that all relevant matters have been covered.

Lisha Chen-Wilson, David Argles, Michele Schiano di Zenise, and Gary Wills discuss the user-centric eCertificate system aimed at supporting the eID system. Although the eCertificate and eID are quite similar in concept, their structures and execution environments are different. According to the authors, an eCert file is a collection of selectable support files, individually signed with references embedded in the main content, before it is signed and encrypted with the access control metadata. On the other hand, the ideal eID file will be a collection of selectable text information with an ID image gathered into a single signed file and encrypted together with the access control metadata. The existing eCert protocol that was initially designed for managing eCertificates in a web environment is not able to manage eID in a mobile environment straightaway.

The authors developed a new eCertificate model which they have adjusted to adapt the new eID file structure, so that it can be recognized by the verification process. The eCertificates can be securely distributed and verified independently from the issuing body and satisfy ownership rights, without requiring storage in the verification system. The innovative model thus creates a newly designed centralized verification service for such digitally signed and access controlled distributed eCertificates.

Electronic Identity is a "must read" book which would be useful for researchers, lawyers, policy makers, technologists, and anyone serious about understanding the challenges of a pan-European eID and how it impacts life online and offline.

Sylvia Kierkegaard

Contents

Chapter 1
Legal Aspects

Norberto Nuno Gomes de Andrade

Abstract This chapter examines the core legal and regulatory issues regarding electronic identity (eID) in the European Union. It is structured into five sections. Section 1.2 explains the terminology employed in the field of eID, defining the main concepts and terms of eID and electronic identity management systems (IDMs). Section 1.3 describes the rising socioeconomic relevance of eID, emphasizing its role as key enabler of economic growth. More specifically, this section assesses the importance of eID for citizens, governments, and business. Section 1.4 examines how eID is currently regulated in Europe, focusing on Directive 1999/93/EC on electronic signatures (eSig directive). Within such analysis, the chapter explains the Directive's current shortcomings and the reasons for the unsuccessful uptake of electronic signatures in the EU. Section 1.5 provides a succinct analysis of the revision process of the eSig directive, which is currently in progress. The chapter outlines the main elements and novelties of the recently proposed Regulation on electronic identification and trust services for electronic transactions in the internal market. This section notes how the scope of the existing eSig directive will be considerably expanded, describing the establishment of a mutual recognition of notified electronic identifications schemes and electronic trust services in the EU. Section 1.6 looks at the main and common objective behind eID regulatory initiatives and projects developed in the EU: the creation of a pan-European eID legal framework. In this context, it elaborates on the obstacles that are hindering the establishment of such scheme. As a way to overcome these obstacles and move forward, the chapter proposes a conceptual framework of principles that could form the basis of a future EU legal framework for the protection and management of digital identities: the principles of user-centricity, anonymity, and pseudonimity, as well as the principles of multiple identities, identity portability, unlinkability and negotiation, among others.

The views expressed in this chapter are purely those of the author and may not in any circumstances be regarded as stating an official position of the European Commission.

N. N. G. de Andrade et al., *Electronic Identity*, SpringerBriefs in Cybersecurity,
DOI: 10.1007/978-1-4471-6449-4_1, © The Author(s) 2014