

UNIVERSITÀ DEGLI STUDI DI CAMERINO

FACOLTÀ DI SCIENZE E TECNOLOGIE

Corso di Laurea Specialistica in Informatica (classe 23/S)

Dipartimento di Matematica e Informatica



**“The e-Government Digital Credentials:
Concepts and Case studies”**

Tesi di Laurea sperimentale
in
Reti degli Elaboratori 2

Laureando

Eleonora Paganelli

Relatore

Ing. Alberto Polzonetti

Correlatore

Prof. Flavio Corradini

Table of Contents

PART I – Preface	1
Chapter 1	1
Structure of the thesis	1
Chapter 2	3
European State of the Art	3
2.1 The vision of a Smart World	7
2.2 The European policies and strategies	8
2.2.1 European Projects about Digital Identity	10
2.2.2 Electronic Identity and Citizen Card Initiatives in Europe	15
2.3 Summary	20
PART II - Digital Identity Management	22
Chapter 3	22
Digital Identity and Anonymity	22
3.1 Human Identity	22
3.2 A first approach to Digital Identity	23
3.3 The Digital Identity Lifecycle	24
3.4 The Need for Digital Identity	27
3.4.1 The Laws of Identity	28
3.4.2 Federated Identity	31
3.4.3 Shortcomings	34
3.4.4 Data Protection	35
3.4.5 Digital Identity in eService Access	38
3.5 Summary	40
Chapter 4	42
Digital Credentials	42
4.1 A Concept for an Extended Digital Identity	43
4.2 Digital Identity Revisited	45
4.2.1 Anonymity and Pseudonymity	47
4.3 Digital Credentials	48
4.3.1 Active Digital Credentials	49
4.4 Elements of an Extended Digital Identity	51
4.4.1 Authentication Certificate	51
4.4.2 Signature Certificate	52
4.4.3 Attribute Certificates	52
4.4.4 Digital Documents	52
4.4.5 P3P Profiles	53
4.4.6 Anonymous and Pseudonymous Credentials	53
4.5 Identity management based on Digital Credentials	54
4.5.1 Profiles	55
4.5.2 Participants	57
4.5.3 Protocols	59
4.6 Use of Credentials in e-government Domain	63
4.7 Overview of the Architecture	65
4.8 Considerations Regarding the Storage of Credentials	68
4.8.1 Brokered Approach versus Credentials on the Citizen’s Device	68
4.8.2 Choice of Personal Device for the Management of the Digital Identity	71
4.9 Summary	72

Chapter 5	73
Identity Management Issues	73
5.1 Identity Management Landscape	73
5.2 Identity Management Model	76
5.3 The Identity Management Framework	78
5.3.1 The e-Government Identity Management Framework	81
5.4 Current Research Areas	83
5.4.1 Trends	84
5.4.2 Issues	87
5.5 Conclusions	89
PART III - Unicam Smart Campus	90
Chapter 6	90
Raffaello's card project	90
6.1 General project overview	90
6.2 Raffaello's Card	91
6.2.1 Smart card distribution architecture	93
6.2.2 Raffaello's Card Management Informative system (RCMIS)	96
6.3 The Raffaello's Card and the Unicam Smart Campus	97
Chapter 7	98
Unicam Smart Campus	98
7.1 General Overview	99
7.2 Smart Campus Advantages	101
7.2.1 Smart Books	102
7.2.2 Smart Schoolrooms	103
7.2.3 The Smart Cafeteria	104
7.2.4 Smart Devices	105
7.2.5 The Smart Sports Center	105
7.2.6 Smart Halls with Information Kiosks	105
7.2.7 Smart Stage	106
7.3 Summary	106
Chapter 8	108
Smart Thesis Case Study	108
8.1 RUP Methodology	108
8.1.1 Architectural analysis: the RUP Elaboration phase	110
8.2 System Description	112
8.2.1 Thesis request steps	112
8.3 Actors definition	113
8.4 Use case diagrams	115
8.4.1 Phase 1 : Request Thesis	115
8.4.2 Phase 2: Bureaucracy	120
8.4.3 Phase 3: Dissertation	121
8.5 Domain Model	122
8.5.1 User Functional Area	124
8.5.2 Front-End Functional Area	124
8.5.3 Back-End Functional Area	125
8.6 Dynamic Model	126
8.6.1 Dynamics one	127
8.6.2 Dynamics two	128
8.7 SmartThesis access	134
8.7.1 The Authentication procedure	135
Chapter 9	141
Conclusions	141
9.1 Summary	141

9.2	Key Findings	142
9.3	Further Research	143
	Appendix A	145
	Bibliography	148

List of Figures

Figure 1 - PRIME Project Overview	11
Figure 2 - GUIDE Project Overview	14
Figure 3 - The FinEID card	15
Figure 4 – Italian Electronic identity card	18
Figure 5- An overview on digital identity card projects in Europe	20
Figure 6 - Digital identity management lifecycle	24
Figure 7 - A summary of Cameron’s ‘Laws’ of identity	29
Figure 8- Digital identity in electronic service access	39
Figure 9- Partial identities of an individual	45
Figure 10- Multi-dimensional Aspects of Identity Information	46
Figure 11- Attribute Aggregations, Relationships and Meta-attributes	47
Figure 12 - High Level Active Digital Credential Model	50
Figure 13– Overview of a Credential Management Platform (CMP)	55
Figure 14 – Overview of architecture components	66
Figure 15 – A network-based approach to credential storage	69
Figure 16 - Identity Management Landscape	74
Figure 17 - Context where identity management operates	75
Figure 18 - Current identity management products and solutions	77
Figure 19 - Identity Management Framework	79
Figure 20 - E-Government Identity Management Framework	82
Figure 21 – Different assurance levels	83
Figure 22 - Raffaello’s Card Layout	92
Figure 23 – Smart Card Distribution Architecture	93
Figure 24 – Smart Card Emission Phase	95
Figure 25 - An overview diagram of the campus card system	100
Figure 26 - An overview diagram of the campus card services	101
Figure 27 - RUP activities	111
Figure 28 – Business Use Case Diagram	113
Figure 29 – System Actors	114
Figure 30 – Request Thesis phases	115
Figure 31 – Use case diagram: Thesis proposed by a Professor	116
Figure 32 – Use case diagram: Thesis proposed by a Student	118
Figure 33 – Use case diagram: Bureaucratic procedure	120
Figure 34 – Use case diagram: Dissertation procedure	121
Figure 35 – General Domain Model Diagram	123
Figure 36 – Class Diagram: Thesis Typology	126

Figure 37 – Statechart Diagram: Dynamic Model	126
Figure 38 – Sequence Diagram: Dynamics one	127
Figure 39 – Sequence Diagram: Dynamics two	128
Figure 40 – Activity diagram: Publish Thesis	129
Figure 41 – Sequence diagram: Request Thesis	130
Figure 42 – Activity diagram: Request Thesis	131
Figure 43 – Activity diagram: Propose Thesis	132
Figure 44 – Activity diagram: Thesis assignment	133
Figure 45 – Sequence diagram: Deliver Thesis	134
Figure 46 – Activity diagram: Authentication	135
Figure 47 – Authentication/Authorization overview	137
Figure 48 – General Use case diagram: Authentication procedure	137
Figure 49 – Use case diagram: Authentication procedure	138
Figure 50 – Sequence diagram: Authentication/Authorization procedure	140

PART I

Preface

Chapter 1

Structure of the thesis

As a guideline to the reader, we briefly outline the structure of the thesis. The thesis comprises nine chapters of which four have an introductory character. They serve to introduce the reader to the concepts of digital identity and digital credentials and provide information concerning technical issues that are necessary for the understanding of subsequent chapters. Then follow five chapters that contain the scientific contributions of the thesis. The chapters are structured as follows:

- **Chapter 1** is the introductory chapter of the thesis.
- **Chapter 2** provides an overview of the European Initiatives about Digital identity Management.
- **Chapter 3** explores key concepts related to digital identity. The terms identity, anonymity and pseudonymity are introduced. We attempt a definition of digital identity and explore the concept of the “digital persona”. Furthermore, methods for the authentication of digital identities are discussed.
- **Chapter 4** proposes a concept for an extended digital identity. The concept comprises pseudonymous credentials as a privacy enhancing technology. We present an architecture design and discuss the infrastructure that is necessary to

support the use of pseudonymous credentials on digital citizen cards. Conceptual issues related to the extended digital identity are explored.

- **Chapter 5** presents the architecture and the design for a prototypical implementation. An Identity management model is introduced and it is schematized into an identity management framework. Further research areas on the Identity management are explored.
- **Chapter 6** presents a regional project about digital citizenship diffusion through the NSC Raffaello. We have analyzed the smart card emission and distribution phases.
- **Chapter 7** introduces the smart campus scenario. The role of the Smart Campus is limited to providing an infrastructure at the user's discretion. In this chapter has been analyzed some "Smart Services" for the Students accessible by Raffaello's card that could be achievable in the University of Camerino, especially at the Computer Science.
- **Chapter 8** analyzes a practical case study at the Unicam Smart Campus, that is the Smart Thesis procedure.
- **Chapter 9** provides keynote findings and the final conclusions.

Chapter 2

European State of the Art

The migration of sociability, business, entertainment, and other activities from the physical world to the virtual world of the Internet has dramatic implications on many fronts. The societal mores, legal structures, and commonly accepted business practices that govern everyday life in the physical world have evolved over thousands of years, and that evolution continues every day. But now we're in the process of translating those structures to the Internet, creating a new place where people can interact. That “place” is radically different from the physical world, one where networked applications combine with ubiquitous connectivity to free transactions, communications, and other activities from physical constraints, thus, creating an entirely new set of requirements.

When it comes to enabling a truly virtual world that can accommodate the breadth and depth of human endeavour, nothing is more important than identity. On the Internet, movement is instantaneous. People, applications, transactions, and data can cross many types of borders via many different paths. At the same time, the security issues associated with a very public and virtual space have become painfully clear as spam, phishing attacks, fraud, and identity theft have become all too common.

Digital identity is the keystone that will ensure that the Internet infrastructure is strong enough to meet basic expectations for not just service and functionality, but

security, privacy, and reliability. That fact is becoming more and more obvious to more and more people every day. But as the Zen master once said, knowing the path and walking the path are two very different things.

How we create, use, store, and verify identity in the Internet context is a complex question, one that transcends both the public and private sectors, and every conceivable business. It raises a large number of thorny issues for society and individuals (not the least of which is privacy), corporations (including the regulation of core operations), and governments (laws, regulations, international treaties). The manner in which these issues are resolved will have a long-term impact on all segments of society and will determine what forms of digital identity will first augment, and then (at least potentially) replace the “official” and “trusted” manifestations of identity on which the physical world relies today. That change will take years, extending past the end of the current decade, involving societal, cultural, business, and political efforts.

How much control individuals will be able to take or will want to takeover their digital identity is the subject of intense debate, for example. Pessimists predict that the intersection of government and commerce will create a surveillance state, one that will make privacy an artifact of the past. Optimists predict the liberation of the individual from both corporate and government control through the use of identity technologies that will put the individual in charge, inverting the traditional relationship between “consumers” and “service providers”. That debate will continue for the foreseeable future as unfolding events pull us in both directions.

Today, much of the activity around digital identity is business-focused. The pressure to compete in a networked world while simultaneously reducing costs is driving companies to integrate business processes and information technology on an increasing scale. Many enterprises are creating inward- and outward-facing systems that tie employees, customers, partners, suppliers, contractors, and other constituents into their business processes, for example. Instead of thinking about individual applications, enterprise IT architects must consider end-to-end business processes that span many boundaries, and how they can integrate the components of IT to support them. These trends are causing wholesale change in IT architectures, moving them to what we at Burton Group call “the virtual enterprise”.