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

ANNO ACCADEMICO 2005/2006

Table of Contents

List of Figures

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 trough 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”.