INTRODUCTION
This book is about security in e-government applications with emphasis on Web services. As e-government applications are coming of age, security has been gradually becoming more demanding a requirement for users, administrators, and service providers. The increasingly more widespread use of Web services facilitates the exchange of data among various e-government applications, and, therefore, paving the way for enhanced service delivery. This volume addresses various aspects of building secure e-government architectures and services and presents the views of experts from academia, policy, and the industry to conclude that secure e-government Web services can be deployed in an application-centric and interoperable way. The chapters of this book have been based on conference papers presented in the context of the eMayor project that aimed at secure interoperable e-government services. This book addresses the narrow yet promising area of Web services aiming at shedding new light to this innovative area of applications. Responding to the challenges previously presented, this book gathers contributions from scholars across Europe, the U.S., and China who present their views on secure e-government Web services. The intended readership for this book includes parties with an ongoing interest in e-government with emphasis on security of e-government applications.

BACKGROUND
The first chapter of this book is an introduction to secure e-government as an area of interdisciplinary interest that sets the stage for what will follow in this volume. The chapters of this volume have been presented in two discreet conferences regarding e-government Security. The first event was a conference entitled Trust and Confidence in a Fast Moving Environment that was presented as part of the activities of the eBusiness Forum Working Group ST-3 (www.ebusinessforum.gr). The objective of this working group has been to address security challenges of eBusiness services, applications, and underlying technologies in a broadband environment. An obvious extension to e-government was deemed necessary in view of the public conference organised on July 2, 2004 in Athens and it was hosted by
the Athens Chamber of Commerce and Industry. Chapters II-X were presented at this conference.

The second event in which Chapters X-XVII were presented was entitled e-government: Towards Electronic Democracy. This international conference was organised on March 2-4, 2005, in Bozen-Bolzano, Italy. In the background of this conference, the European Science Foundation (ESF) has established the program, Towards Electronic Democracy (TED), with the overall objectives:

- To discuss and evaluate how advances of interactive decision-analytic tools might help develop e-democracy.
- To develop e-government systems which involve their citizens more fully in the public decision making process.

This conference on interdisciplinary methods and techniques addressed a large spectrum of issues that are relevant and have to be investigated for a successful transition from the traditional form of government to e-government. The conference had a strong interdisciplinary character and brought together people from different sectors, including researchers, technology providers, administrative staff, and politicians. This conference was initiated by the TED working group of the ESF and jointly organized with the Free University of Bozen-Bolzano, the City of Bozen-Bolzano, and the IFIP WG 8.5-Information Systems in Public Administration.

Both conferences belong to a broader initiative that aims at presenting a holistic approach on the design and use of secure and interoperable cross border e-government services in such areas as digital certificates, electronic invoicing, electronic procurement, etc. Experiences, case studies, lessons learned, and best practices are presented by various real life stakeholders that include municipalities, Chambers of Commerce, and Industry, as well as service providers. These views underline the services that have been adopted, reveal barriers, and propose potential solutions and measures that could assist adopting e-government services and increasing the level of privacy and trust in transactions with the European public sector.

**BOOK LAYOUT**

The following chapters were presented at the first conference in the Athens workshop.

Chapter I is a brief introduction to the area of secure e-government. Secure e-government has emerged as a critical goal for public administrations worldwide. While e-government services bring the promise of efficient online services closer to its intended beneficiaries, being citizens, organizations, and other public administration units, new challenges pose potential threats. Emphasis is placed on the evolution of Web services and security technologies as a plausible technology upon which e-government services can be based.
Chapter II focuses on the interoperability aspects of e-government. Research into initiatives worldwide show that some of the legal and organizational barriers for the adoption of new technologies in e-government have largely been addressed. Some additional prevailing requirements for e-government, however, challenge e-government architects. The authors consider Web services and PKI prominent ways to resolve these remaining issues. This chapter presents three innovative e-government services based on these technologies with emphasis on security and interoperability.

Chapter III introduces the notion of trust as a means to establish security in ubiquitous mobile applications. Burmester argues that while trust is an essential enabler of security in open networks, its role is exacerbated in ad hoc wireless environments where there is no network topology. In these networks, communication can be effected through trusted routes. It is therefore important to understand the limitations of such environments and to seek ways to support explicit or implicit trust. Burmester concludes by presenting several models that enable trust based on economic, insurance, information flow, and evolutionary paradigms.

Chapter IV argues that information society is increasingly dependent on distributed systems and infrastructures for critical functions. The increasing complexity of these systems is rapidly growing along with the pervasive use of open information infrastructures for applications and communications. For Servida, this trend exposes society to cyber vulnerabilities and threats that require control. This chapter outlines the main research directions that have are priority in EU research programmes.

Chapter V examines broadband communication networks and the repercussions of their excess capacity. In specific location-based services over wireless broadband networks are gradually becoming more widespread in an emerging ambient intelligence society. Location-based services over broadband and peer-to-peer networks user authentication ensures trust. Biometric authentication is an approach to providing irrefutable identity verification of a user, thus providing the highest level of security. This chapter addresses some of the issues associated with the use of biometric identity for user and device authentication over broadband wireless networks.

Chapter VI presents an application centric overview of a topical case study. The liberalization of the energy market requires frequent online access to metering devices that is necessary for exchanging meter data. Integrating security is an essential requirement for online meter device access. Ruland presents the SELMA project (Secure Electronic Exchange of Metering Data) and emphasises on the security aspects and claims that the security concept includes the security mechanisms and cryptographic techniques applied to the metering data as well as the security management.

Chapter VII addresses reliable enforcement of security policies for e-government. While e-government organizations interact frequently with citizens and/or businesses to deliver paper-based and electronic services, they also interact also with each other in various contexts. The authors identify a clear need for a secure,
interoperable, and cost-effective e-government platform that addresses the require-
ments of small e-government organizations.

Chapter VIII claims that the use of electronic technologies in e-government adds up to end user convenience in spite of the security threats that steel hamper its widespread use. Denial of service attacks are becoming an increasingly alarming a factor in e-government that highlights the seriousness of the situation. To limit the impact of denial of service attacks, the authors claim that the use of best practices along with a classification of attacks and defence mechanisms can lead to a resolu-
tion of the problem.

Chapter IX claims that secure e-government aims at supporting public ad-
ministration in delivering enhanced public services. In e-government, electronic signatures and certification services are used to invoke trust and security in services and applications. The author sees a risk in certification services that if being on offer in an apparent geographical or contextual isolation threaten to create fault lines across e-government services. Limitations in interoperability of certification services might hamper trust and security in the whole value chain of e-government applications. Drawing from the case of small public administrations the author proposes a certification service architecture and approach to support interoperability in secure e-government services.

The following chapters were presented at Towards Electronic Democracy Conference, Bolzano, March 2005.

Chapter X addresses the widespread diffusion of online services provided by public and private organizations driven by e-government applications highlights the need for user authentication and authorisation. Single sign on technology combined with strong authentication meets the requirement of protecting against replay attacks. Additionally, PKI and digital identity concepts are presented in the framework of the PRIME project to conclude that multiple dependable identities that are needed in modern day transactions as a general solution for identity management has yet to come.

Chapter XI addresses ePolling systems that are a critical component in e-de-
mocracy services. In e-polling systems, security requirements remain a high level in spite of their acceptance error that does not affect the final result. This chapter proposes a protocol for accurate and anonymous ePolling in which trust is presented in a measurable way by permitting voters to verify that their casted votes have been counted.

Chapter XII presents a methodology for proving in zero knowledge, the validity of selecting a subset of a set belonging to a predefined family of sets. Applying the proposed methodology to electronic voting the authors can provide for extended ballot options. This chapter claims that complexity is linear with respect to the total number of participants in an election.

Chapter XIII addresses the issue of orchestrating secure and dependable e-government services by linking them at request. The chapter investigates the applicability of two existing reference models, the workflow reference model and the extended SOA reference model. This chapter makes recommendations toward
ensuring correct and in-time service-delivery processes, secure information sharing, and transparent and accountable processes.

Chapter XIV presents model driven architecture, an approach to increase the quality of complex software systems by creating high-level system models and automatically generating system architectures and components. This chapter shows how this paradigm can be applied to model driven security for inter-organizational workflows in e-government. While the focus is on the realization of security critical inter-organizational workflows in the context of Web services, security requirements are specified at an abstract level using UML diagrams to produce security relevant artifacts for the target reference architecture based on Web service security standards.

Chapter XV seeks to sustain the quality of e-government services and solve the problem of efficient and secure electronic exchange and processing of governmental documents and data. The authors consider that a major difficulty in a distributed deployment is the heterogeneity of interconnected systems that are required operating in multiple organizational domains. This chapter presents how the ISO/RM-ODP standard offers a general framework to design and develop an open distributed system attuned to e-government, including a high-level case study of how this standard can be applied in system design in e-government.

Chapter XVI introduces the goal of ShanghaiGrid and its sub-project, e-government on the grid. This chapter asserts that the main existing problem of e-government is how to integrate each government agency’s resources to form cross-agency services. A grid technique provides an ideal way to solve this problem while workflow middleware and a real-name citizen mailbox are also presented.

Chapter XVII proposes a new concept of e-government service marketplace (e-govSM). This chapter presents an overview of the architecture and implementation of e-govSM easing the automation of administrative processes involving several administrations and allowing the reuse of data. This architecture facilitates citizens’ interaction with various public administrations by providing them a single and personalized access point to services. The e-govSM is formalized using a set of XML schema models to support an interoperable and open system. The architecture is based on four main functional modules for the creation and management of citizen unique identifiers, for the management of citizen interactions with the marketplace, for the management of administrative process execution, and for the management of all public administrations interactions with e-govSM.

NOTE

Nothing in this Preface or book may be interpreted or construed as representing the views and opinion of any other party except the authors of the chapters herein in any way whatsoever. The editors acknowledge that this volume represents their personal efforts; the opinions expressed herein do not represent the views of any third party including the editors’ employers past or present in any way whatsoever.