# Secure Multi-Party Non-Repudiation Protocols and Applications

# Secure Multi-Party Non-Repudiation Protocols and Applications

*by*

José A. Onieva
*University of Malaga*
*Spain*

Javier Lopez
*University of Malaga*
*Spain*

Jianying Zhou
*Institute for Infocomm Research*
*Singapore*

Springer

Authors:
José A. Onieva
University of Malaga
Computer Science Dept.
E.T.S. Ingenieria Informaica
Campus de Teatinos
29071 Malaga, Spain
onieva@lcc.uma.es

Javier Lopez
University of Malaga
Computer Science Dept.
E.T.S. Ingenieria Informaica
Campus de Teatinos
29071 Malaga, Spain
jlm@lcc.uma.es

Jianying Zhou
Institute for Infocomm Research (12R)
21 Heng Mui Keng Terrace
Singapore 119613, Singapore
jyzhou@i2r.a-star.edu.sg

ISBN-13: 978-0-387-75629-5 e-ISBN-13: 978-0-387-75630-1

Library of Congress Control Number: 2008938604



Printed on acid-free paper

springer.com

*To my parents, for being always there.*
*– Jose A. Onieva.*

# Preface

Currently, it seems that each day the world is less reluctant to accept the truth: communications will be shifted to Internet (whatever the generation is when it takes place). Doubtlessly, this will result in a large number of advantages, speeding up the way we have to make businesses and be in touch with each other. Some solutions are already part of our lives and either enhance or provide new methods for communicating, purchasing, selling, reporting and in general transmitting information. Some of these are: VoIP, Instant Messaging, E-Mail, E-commerce, Internet Payment methods, P2P for file sharing, etc.

In some of these methods efficiency and functionality are of major concern. Furthermore, tools (or protocols) providing this functionality have gained a place or become a de-facto standard because they perform better at providing this key components. Nevertheless, other solutions need to consider security as a key component from the very beginning of their design. Moreover, fulfilling this important and at the same time difficult to achieve property, some solutions have failed to accomplish their purpose as users are still unenthusiastic about adopting new solutions if either security is important or otherwise this is not provided with a 100% assurance. In other words, trust is not easily assumed by users in e-payment methods, e-commerce, e-banking, contract signing applications, Internet biddings, etc.

But as security practitioners learn from the very beginning of their career, there's no unconditional and complete secure system. What's more, it will never exist. There is always something that could not work in the system, be broken up, accessed without authorization, leaked information, etc. And if not, the human component (which will be present as long as we do) would need to be totally trusted not to put in risk all the implemented security measures.

This is the reason for which in traditional paper-based procedures (as with contract signing, money transfers, etc.) accountability as a means to solve possible disputes among users has always played part of the procedure itself. Here the handwritten signature plays the main role. It allows for (non-)repudiation of acts such that, for instance, a bank cannot transfer our money from one account to another if it does not have an application with our consent (signature). And of course, it exists

the digital counterpart: the digital signature. And even better, most of the countries already (or are in the way to) have legislated its use.

But unfortunately, the network communication grounds (and among them, distance and lack of trust) make translation of paper-based procedures to networked digital ones hard to achieve. Thus, in order to realize security in Internet (or any other networked including mobile) applications, special protocols are needed to ensure that any dispute could be solved between users if the network fails or an entity misbehaves. In the computer security field, these protocols are known as non-repudiation protocols.

Research oriented to non-repudiation protocols has been active since late 90's; considering in most occasions Alice and Bob as the players of the protocol design scenario. It is time to give a step forward and realize that in many applications there are more than two entities and that two-party protocols are not appropriate for scenarios in which multiple entities are involved. This is the main aim of this book.

This book is mainly targeted to professional audiences with in-depth knowledge of information security and a basic knowledge of applied cryptography. This book briefly settles the state of the art in non-repudiation protocols and gives insight of its applicability to e-commerce applications. It organizes the existing scant literature regarding non-repudiation protocols with multiple entities' participation. It provides to the reader with sufficient grounds to understand the non-repudiation property and its applicability to real applications. Security practitioners will find it very useful in the design of secure applications with multiple entities, helping them to envisage the basics of multi-party non-repudiation as a necessary tool when trust is not present among players. Additionally it could serve as text book for postgraduate students who wish to understand the non-repudiation service and mechanisms in the presence of an undefined number of players.

Malaga,
September 2008

*Javier Lopez*
*Jianying Zhou*
*Jose A. Onieva*

# Contents

# List of Figures

# List of Tables

# Acronyms

Lists of abbreviations, symbols.

| | |
|---|---|
| ANX | Automotive Network Exchange |
| API | Application Programming Interface |
| B2B | Business-to-Business |
| B2C | Business-to-Consumer |
| C2C | Consumer-to-Consumer |
| CA | Certification Authority |
| CEM | Certified Electronic Mail |
| CEMBS | CErtificate of a Message Being a Signature |
| CRL | Certificate Revocation List |
| DES | Data Encryption Standard |
| DoS | Denial of Service |
| DRM | Digital Rights Management |
| DSA | Digital Signature Algorithm |
| DSS | Digital Signature Standard |
| EOD | Evidence of Delivery |
| EOO | Evidence of Origin |
| EOR | Evidence of Receipt |
| ERP | Enterprise Resource Planning |
| EU | European Union |
| FTP | File Transport Protocol |
| GPRS | General Packet Radio Service |
| HTML | HyperText Markup Language |
| HTTP | HyperText Transfer Protocol |
| HTTPS | Secure HyperText Transfer Protocol |
| IETF | Internet Engineering Task Force |
| IN | Intermadiary ageNt |
| IP | Internet Protocol |
| IPSec | Internet Protocol Security |
| ISO | International Standarization Organization |

| | |
|---|---|
| IT | Information Technology |
| ITU | International Telecommunications Union |
| L2TP | The Layer Two Tunneling Protocol |
| LAN | Local Area Network |
| MPNR | MultiParty Non-Repudiation |
| MAC | Message Authentication Code |
| MNO | Mobile Network Operator |
| MPCS | Multi-Party Contract Signing |
| NRD | Non-repudiation of Delivery |
| NRO | Non-Repudiation of Origin |
| NRR | Non-Repudiation of Receipt |
| NRS | Non-repudiation of Submission |
| OCSP | On-line Certificate Server Protocol |
| ODR | On-line Dispute Resolution |
| OMA | Open Mobile Alliance |
| OS | Operating Systems |
| OSI | Open System Interconnection |
| P2P | Peer-to-Peer |
| PC | Personal Computer |
| PCS | Private Contract Signature |
| PDA | Personal Digital Assistant |
| PGP | Pretty Good Privacy |
| PKI | Public Key Infrastructure |
| PPTP | Point-to-Point Tunneling Protocol |
| PRAC | Partial Result Authentication Code |
| QES | Qualified Electronic Signature |
| QoS | Quality of Service |
| RSA | Rivest, Shamir and Adelman |
| RO | Right Object |
| RI | Rights Issuer |
| SET | Secure Electronic Transaction |
| SHA | Secure Hash Algorithm |
| SSL | Secure Socket Layer |
| SSH | Secure SHell |
| S/MIME | Secure/Multipurpose Internet Mail Extensions |
| TSA | Time-Stamp Authority |
| TCP | Transport Control Protocol |
| TLS | Transport Layer Security |
| TPD | Trusted Personal Device |
| TTP | Trusted Third Party |
| URL | Uniform Resource Locator |
| VPN | Virtual Private Network |
| WEP | Wireless Equivalent Privacy |
| WTLS | Wireless Transport Layer Security |
| XML | eXtensible Markup Language |