Secure Web Services Protocol for Fair Contract Signing with Off-line Semi-Trusted Third Party

Wu Zongjie, Cao Weijun
E-mail: 9314379@mail.dyu.edu.tw

ABSTRACT

Fairness becomes a key factor while a data exchange since the transaction is conducted over the Internet. To start the data exchange, confidential data, payments, and signatures need to be transmitted. Main parties are afraid of they cannot get electronic documents from the other side safely while the data exchange. To ensure the fairness of data exchange, the protocol needs a trusted third party be a judge when the dispute occurs, and has to give a guarantee to main parties during the data exchange. Online contract signing is a kind of fair exchange. In addition to traditional contract signing, online contract signing has become a flexible method in business. Online contract signing consists of three main parties, including two signers and trusted third party. Currently, in the studies, most of the third parties are either online semi-trusted third party or off-line trusted third party. To eliminate the third party's connectional time and enhance its security, a secure and efficient protocol for fair contract signing with off-line semi-trusted third party has proposed in the proposed protocol, where a flexible method for selecting a semi-trusted third party is proposed actually. The online contract signing is still fair while the third party is off-line and main parties can rely on the semi-trusted with third party. Finally, in the thesis, the proposed protocol is extended to Web services so that it can be used for main parties in different platforms.

Keywords : Fair Data Exchange, Online Contract Signing, Off-line Semi-Trusted Third Party, Web Services

Table of Contents

Chapter I. INTRODUCTION 1
1.1 Background and Motivation 1
1.2 Purpose 4
1.3 Scope 4
1.4 Research Procedure 5
1.5 Thesis Organization 7

Chapter II. PREVIOUS WORKS 8
2.1 Fair Exchange 8
2.2 Contract Signing 9
2.3 DSS-Based Signature 10
2.2.1 Signature Generation 12
2.2.2 Signature Verification 13
2.4 Group-Oriented Digital Multisignature Scheme 14
2.5 XML Security 16
2.5.1 XML Digital Signature 16
2.5.2 XML Encryption 20
2.6 Web Services 22
2.6.1 SOAP 24
2.6.2 XKMS 26
2.7 WS-Security 29

Chapter III. RESEARCH METHODS 30
3.1 Semi-Trusted Third Party Selection Phase 30
3.2 Normal Phase-Signature Verification 32
3.3 Normal Phase-Contract Signing 33
3.4 Dispute Phase 34
3.1.1 Case I: dispute in party B 35
3.1.2 Case II: dispute in party A 36

Chapter IV. PROPOSED PROTOCOL FOR WEB SERVICES 38
4.1 Semi-Trusted Third Party Selection Phase 38
4.2 Normal Phase- Signature Verification 41
4.3 Normal Phase-Contract Signing 44
4.4 Dispute Phase 47
4.4.1 Case I: dispute in party B 47
4.4.2 Case II: dispute in party A 50

Chapter V. SECURITY ANALYSIS AND PERFORMANCE EVALUATION 53
5.1 Security Analysis 53
5.1.1 A semi-trusted third party 53
5.1.2 Scenarios 53
5.1.3 Completeness and Privacy 54
5.1.4 WS-Security 55
5.2 Performance Evaluation 55
5.3 Comparisons 56

Chapter VI. CONCLUSIONS 59

BIBLIOGRAPHY 61

REFERENCES


DSS-Signature, www.itl.nist.gov/fipspubs/fip186.htm
XML Encryption, www.w3.org/TR/xmlenc-core/
XML Signature, www.w3.org/Signature/
XKMS, www.w3.org/TR/xkms2/