

Efficient and Secure Card-based Payment System

Based on ANSI X9.59-2006

By

CHEONG CHI PO

Master of Science in E-Commerce Technology

2007



Faculty of Science and Technology

University of Macau

Contents

Abstract.....	iii
List of Figures	viii
List of Tables.....	ix
Chapter 1 Overview of Electronic Payment Systems	1
1.1 The Roles of Electronic Payment Systems	1
1.2 Motivations of Electronic Payment Systems.....	2
1.3 Types of Electronic Payment Systems	3
1.4 Backgrounds of Card-Based Electronic Payment Systems.....	4
1.5 Objectives and Plans	5
Chapter 2 Overview of Electronic Card-based Payment Systems	6
2.1 Electronic Vs Traditional Payment System.....	6
2.2 Traditional Card-based Payment System	7
2.2.1 Payment flow	7
2.2.2 Overview of ISO 8583 financial messages.....	8
2.3 Participants in Card-based Electronic Payment System	9
2.3.1 Trust relationship.....	10
2.4 Types of Card-based Electronic Payment Systems.....	11
2.5 Methodology and Evaluation Factors	12
2.5.1 Identification	13
2.5.2 Confidentiality	14
2.5.3 Integrity	14
2.5.4 Non-repudiation	14
2.5.5 Interoperability	15

2.5.6 Easy to use in both cardholder and merchant side	15
2.5.7 Easy implementation in consumer and merchant's computer	15
2.6 Description of Existing Problems	15
Chapter 3 Research on Electronic Card-based Payment Systems	17
3.1 First Virtual (FV)	17
3.2 CyberCash	19
3.3 PKI based Payment Protocol – iKP, SEPP, SET	21
3.3.1 iKP	21
3.3.2 SEPP	22
3.3.3 SET	22
3.4 Visa 3D Protocol	25
3.5 Secure Socket Layer	27
Chapter 4 Overview of Account Based Payment Object - ANSI X9.59-2006	29
4.1 Motivations of Account Based Digital Signature	29
4.2 Architecture of ANSI X9.59-2006	31
4.3 Secure Payment Objects in X9.59	31
4.4 Basic Payment Flow	32
4.5 Mappings between X9.59 and ISO 8583	35
4.6 The Advantages and Disadvantages of X9.59	36
4.6.1. Advantages of X9.59	36
4.6.2 Disadvantages of X9.59	37
Chapter 5 Efficient and Secure Card-based Payment System based on ANSI X9.59-2006	38
5.1 Scope of ESCPS	38
5.2 ESCPS Payment Flow	39
5.3 Signed Objects Defined in ESCPS	41
5.4 Security Services	46
5.4.1 Confidentially	46
5.4.2 Authentication	47
5.4.3 Integrity	47
5.5 Advantages of ESCPS	47
Chapter 6 System Design of ESCPS	49

6.1 Typical Electronic Credit Card Payment Model and Architecture	49
6.2 The Architecture of the ESCPS	51
6.2.1 The Use of the Web Services	54
6.3 Classes Design in ESCPS.....	55
6.4 The Event Flow of the ESCPS	56
6.5 The Messages of ESCPS	57
6.5.1 Message header	58
6.5.2 Signed objects	59
Chapter 7 Performance Evaluation	64
7.1 Simulation	64
7.2 Modeling and Analysis Method.....	65
7.3 System Parameters	66
7.4 Assumptions of the Model.....	68
7.5 Building the SET Simulation Model.....	68
7.6 Building the X9.59 Simulation Model.....	71
7.7 Building the ESCPS Simulation Model	72
7.8 Results of Performance Evaluation.....	73
Chapter 8 Conclusion	78
Appendix A Hash and Cryptography Algorithms.....	80
Appendix B Associated Publications.....	87
References.....	88