List of Figures

1.1 Single CA PKI architecture ........................................ 7
1.2 Hierarchical PKI architecture ..................................... 8
1.3 Multi-rooted PKI architecture .................................... 9
1.4 Mesh PKI architecture ............................................. 10
1.5 Hybrid PKI architecture .......................................... 11
1.6 Bridge PKI architecture .......................................... 11
1.7 GWCA PKI architecture ........................................... 12
1.8 X.509 Certificate Format .......................................... 14
1.9 Basic structure of Certificate Revocation List .................. 16
1.10 OCSP Components’ Interaction ................................. 17

2.1 Digital Signature Generation and Verification.................. 27

3.1 Merged Hierarchical PKIs with cross-certifications .......... 47
3.2 Merging Hierarchical PKIs by introducing new CA .......... 48
3.3 Merging Hierarchical PKIs without using cross-certification .. 50
3.4 Merging Hierarchical PKIs during acquisition of companies . 51

4.1 The overall process diagram of the proposed merging process . 62
4.2 A certificate structure ............................................ 67
4.3 Work flow diagram for hierarchy creation ...................... 69
4.4 Merging Hierarchical PKIs without using cross-certification . 70
4.5 Certificate path verification time in normal method (cross-certification at the root) and the proposed method ................................. 72

5.1 PKIs before merging with cross-certification ................................. 78
5.2 PKIs after Merging with cross-certification ................................. 79
5.3 PKIs after Acquiring ......................................................... 80
5.4 The overall process diagram of the proposed merging process ........... 81
5.5 Input PKIs ................................................................. 83
5.6 Merged PKI with RCA2 as new Root CA ($RCA_{new}$) and same certificate Policies ......................................................... 84
5.7 Merged PKI with RCA2 as new Root CA ($RCA_{new}$) and different certificate Policies ......................................................... 84

6.1 Flowgraph of the parsing process ............................................ 95
6.2 Tree structure representing a certificate policy ............................... 97

7.1 The Hierarchical PKI ......................................................... 109
7.2 Path Validation Outline ....................................................... 114
7.3 Conversion of Hierarchical structure to a binary tree ......................... 122
7.4 Path Verification time with Forward and Reverse path constructions 124
7.5 The process diagram for the proposed path verification method ........... 127
7.6 Normal method vs. Proposed method with 25%, 50% and 75% cache hit ......................................................... 129

8.1 Cross-Certified Mesh Architecture ........................................... 131
8.2 A Mesh Network with multiple paths between users ......................... 135
8.3 A Mesh PKI and its equivalent DFS spanning tree ............................ 136
8.4 A single collective ......................................................... 137
8.5 An emerging hierarchy ...................................................... 137
8.6 A Mesh PKI ................................................................. 141
8.7 Constructing the hierarchy where node 6 chooses node 7 as a superior node ........................................ 143
8.8 Constructing the hierarchy where node 2 chooses node 4 as a superior node ........................................ 143
8.9 Constructing the hierarchy where node 3 chooses node 4 as the superior node ........................................ 144
8.10 Constructing the hierarchy where node 1 chooses node 5 and node 8 as its superior node ......................... 144
8.11 Established Multi-rooted Hierarchical structure ......................... 145