

# CONTENTS

1 INTRODUCTION	5
1.1 Benefits of biometrics	5
1.2 Key biometric terms	5
1.3 Error classification and performance evaluation	7
1.4 Goals of this work	8
2 ACTUAL STATE	9
2.1 Problem definition	9
2.1.1 Fingerprint acquisition	9
2.1.2 Fingerprint classification	9
2.1.3 Fingerprint matching	10
2.2 Fingerprint recognition algorithms	10
2.2.1 Fingerprint enhancement	11
2.2.2 Fingerprint classification	11
2.2.3 Minutiae extraction	12
2.3 Actual solutions	12
2.3.1 Fingerprint technology	12
3 STRENGTH OF FINGERPRINT INFORMATION	13
3.1 Basics of entropy and attack possibilities	13
3.1.1 Shannon's theory	13
3.1.2 Entropy	13
3.1.3 Pseudorandom bits and sequences	14
3.2 Uniqueness of fingerprints	14
3.2.1 Fingerprint uniqueness model	14
3.2.2 Experimental results	15
3.3 Strength of information from fingerprints	15
3.3.1 Resolution	15
3.3.2 Fingerprint size	15
3.3.3 Minutia and antiminutia	15
3.3.4 Strength of information contained in fingerprints	16
3.3.5 Vector quantization	17
3.3.6 Key length	17
3.3.7 Summary of fingerprint information strength	18
4 KEY GENERATION	19
4.1 Biometric security system	19
4.2 Certificate creation concept	19
4.2.1 Acquirement phase	20
4.2.2 Key generation phase	22
4.2.3 Cryptomodule phase	24

4.3 Certificate usage concept	24
4.3.1 Acquirement phase	24
4.3.2 Key generation phase	24
4.3.3 Cryptomodule phase	25
4.4 Proposal of practical usage	25

## 5 PRACTICAL RESULTS AND SUMMARY 26

5.1 Fingerprint database	26
5.2 Database enrollment and matching (industrial algorithms)	26
5.3 Key generation	26
5.4 Future work	29

## 6 REFERENCES 30