
TABLE OF CONTENTS

Abbreviations		VII
One	Introduction	1
1.1	Introduction	3
1.2	Defining the Problem	4
1.3	Outline	6
Two	Authentication Technology: an Elementary Explanation	9
2.1	Introduction	11
2.2	Authentication Within the Internet	11
2.3	Dedicated Means of Authentication	15
2.4	Public Key Encryption	25
2.4.1	Public key encryption in general	25
2.4.2	Certification	28
2.4.3	PKI-based authentication mechanisms	41
2.4.4	Technologies covering partial aspects	49
Three	Usability of Authentication Technology	53
3.1	Introduction	55
3.2	Qualification as a Signature	55
3.2.1	Forms of recognition	55
3.2.2	The functions of a signature	59
3.2.3	Performing the functions with the help of technology	71
3.2.3.1	Technologies for network identification	72
3.2.3.2	Passwords and PINs	73
3.2.3.3	Biometric technology	74
3.2.3.4	Symmetric encryption	76
3.2.3.5	Digital signatures	77
3.2.3.6	SSL and TLS	79
3.2.3.7	Timestamps and Cards	80

3.2.4	The functions of and qualification as a signature	80
3.2.5	What is beyond functional equivalence?	81
3.3	Evidentiary Value	89
3.4	Semi-legal Considerations of Usability	94
Four	Misuse and the Burden of Proof	99
4.1	Introduction	101
4.2	The Division of Risks	101
4.3	The Division of the Burden of Proof	111
Five	Privacy Implications of the Use of Electronic Signatures	117
5.1	Why Privacy?	119
5.2	Digital Signatures	121
5.2.1	Personal data?	121
5.2.2	The processing of personal data	123
5.3	Symmetric Encryption	125
5.4	Biometrics: the Dynamic Signature or Signature-scan	126
5.5	Conclusion	128
Six	Conclusion	131
	Literature	143
	Appendix	147
	Index	148