

ISO/IEC 14888-2:2008-04 (E)

Information technology - Security techniques - Digital signatures with appendix - Part 2: Integer factorization based mechanisms

Contents		Page
Foreword		iv
Introduction		v
1 Scope		1
2 Normative references		1
3 Terms and definitions		1
4 Symbols and abbreviated terms		2
5 General		4
6 RSA and RW schemes		7
7 GQ1 scheme (identity-based scheme)		11
8 GQ2 scheme		15
9 GPS1 scheme		18
10 GPS2 scheme		21
11 ESIGN scheme		23
Annex A (normative) Object identifiers		27
Annex B (informative) Guidance on parameter choice and comparison of signature schemes		33
Annex C (informative) Numerical examples		41
Annex D (informative) Two other format mechanisms for RSA/RW schemes		56
Annex E (informative) Products allowing message recovery for RSA/RW verification mechanisms ..		59
Annex F (informative) Products allowing two-pass authentication for GQ/GPS schemes		61
Bibliography		65