

ISO/IEC 23264-2:2024-08 (E)

Information security - Redaction of authentic data - Part 2: Redactable signature schemes based on asymmetric mechanisms

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Symbols and conventions	3
4.1	Symbols	3
4.2	Conventions	4
5	General	5
6	Generic construction from signature schemes and hash-functions	5
6.1	Parameters	5
6.2	Construction	6
6.2.1	Key generation process	6
6.2.2	Redactable attestation process	6
6.2.3	Redaction process	7
6.2.4	Verification process	8
7	Scheme SBZ02-MERSAProd	8
7.1	Parameters	8
7.2	Construction	9
7.2.1	Key generation process	9
7.2.2	Redactable attestation process	9
7.2.3	Redaction process	10
7.2.4	Verification process	11
8	Scheme BBDFFKMOPPS10	12
8.1	Parameters	12
8.2	Construction	12
8.2.1	Key generation process	12
8.2.2	Redactable attestation process	12
8.2.3	Redaction process	14
8.2.4	Verification process	15
9	Scheme DPSS15	17
9.1	Parameters	17
9.2	Subroutine: RSA Accumulators	17
9.3	Construction	18
9.3.1	Key generation process	18
9.3.2	Redactable attestation process	19
9.3.3	Redaction process	20
9.3.4	Verification Process	20
10	Scheme MHI06	21
10.1	Parameters	21

10.2	Construction	22
10.2.1	Key generation process	22
10.2.2	Redactable attestation process	22
10.2.3	Redaction process	23
10.2.4	Verification Process	24
11	Scheme MIMSITI05	25
11.1	Parameters	25
11.2	Construction	25
11.2.1	Key generation process	25
11.2.2	Redactable attestation process	25
11.2.3	Redaction process	26
11.2.4	Verification Process	27
Annex A (normative)	Objectidentifiers	29
Annex B (informative)	Overview of properties of redactable signature schemes based on asymmetric mechanisms	30
Annex C (informative)	Criteria for inclusion of schemes in this document	33
Annex D (informative)	Numerical examples	34
Bibliography		57