

ISO/IEC 20009-4:2017-08 (E)

Information technology - Security techniques - Anonymous entity authentication - Part 4: Mechanisms based on weak secrets

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Symbols, abbreviated terms and conversion functions	4
4.1	Symbols and abbreviated terms	4
4.2	Conversion functions	7
5	General model for password-based anonymous entity authentication	7
5.1	Participants	7
5.2	Types of PAEA mechanisms	7
5.3	Components of a password-only PAEA	7
5.4	Components of a storage-extra PAEA	8
5.5	Operation of a PAEA	8
6	Password-only PAEA mechanisms	9
6.1	General	9
6.2	SKI mechanism	9
6.2.1	Setup	9
6.2.2	User registration	10
6.2.3	Anonymous authentication	10
6.2.4	User revocation	12
6.3	YZ mechanism	12
6.3.1	Setup	12
6.3.2	User registration	12
6.3.3	Anonymous authentication	13
6.3.4	User revocation	14
7	Storage-extra PAEA mechanism	14
7.1	General	14
7.2	YZW mechanism	14
7.2.1	General	14
7.2.2	Setup	15
7.2.3	User registration	15
7.2.4	Anonymous authentication	16
7.2.5	User revocation	17
Annex A (normative)	Object identifiers	19
Bibliography		20