

ISO/IEC 19286:2018-01 (E)

Identification cards - Integrated circuit cards - Privacy-enhancing protocols and services

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Abbreviated terms and notations	5
5	General privacy principles	6
5.1	General	6
5.2	Data minimization	7
5.3	User control	7
5.4	Data quality	7
6	Privacy architecture	8
6.1	General	8
6.2	Categorization of data	9
6.2.1	User data and credentials	9
6.2.2	User input data	10
6.2.3	ICC data	10
6.2.4	Service provider data (SP data)	10
6.2.5	Issuer data	10
6.3	Participating entities	11
6.4	Privacy properties	11
6.4.1	Data minimizing properties	11
6.4.2	User control properties	12
6.4.3	Data quality properties	13
7	Privacy-enhancing protocols	14
7.1	General	14
7.2	User verification	15
7.2.1	Purpose of user verification	15
7.2.2	Password verification with VERIFY command	15
7.2.3	Password verification with PACE	17
7.2.4	Biometric user verification	20
7.3	Device authentication protocols with optional user attribute access	22
7.3.1	Purpose of device authentication protocols	22
7.3.2	Authentication protocol PACE	22
7.3.3	Authentication protocol EACv2 with on-card user attributes	24
7.3.4	ABC protocol with on-card user attributes	30
7.3.5	Enhanced Role Authentication protocol (ERA)	34
7.3.6	Device authentication protocol OPACITY Full Secrecy	41
7.3.7	Device authentication protocol OPACITY BLINDED	43
7.4	Attribute verification mechanisms with compare command	45
7.4.1	Purpose of attribute verification mechanism	45
7.4.2	General	45
7.4.3	Data comparison with external authentication function	46

7.4.4	Auxiliary data comparison with EACv2 protocol	47
7.5	Domain-specific identifier mechanisms	49
7.5.1	Purpose of domain-specific identifier mechanisms	49
7.5.2	Domain-specific identifier based on Restricted Identification	49
7.5.3	Domain-specific identifier based on pseudonymous signature for authentication	51
7.5.4	Domain-specific identifier based on ABC-based signatures	52
7.6	Pseudonymous signature mechanisms	52
7.6.1	Purpose of pseudonymous signatures	52
7.6.2	Chip Authentication based on Pseudonymous Signature for Authentication (CA-PSA).....	52
7.6.3	Pseudonymous Signature of Credentials (PSC)	55
7.6.4	ABC-based signatures (ABC-Sig)	56
Annex A (informative) Use cases		59
Annex B (informative) Privacy Impact Assessment (PIA) guidance for electronic identification, authentication and trust services		64
Bibliography		75