

ISO/TS 12812-2:2017-03 (E)

Core banking - Mobile financial services - Part 2: Security and data protection for mobile financial services

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	2
4	Abbreviated terms	4
5	Summary of the technical nature of the clauses	5
6	Security management considerations	7
6.1	General	7
6.2	Three-layer model to manage security for mobile financial services	8
6.2.1	Process layer	9
6.2.2	Application layer	10
6.2.3	Infrastructure layer	10
7	Security principles and minimum requirements for mobile financial services	11
7.1	Security architecture aspects to be considered	11
7.2	Mobile financial services hardening techniques overview	13
7.2.1	General	13
7.2.2	Mobile device hardening techniques overview	13
7.2.3	Wireless networks hardening techniques overview	13
7.2.4	Secure remote management of mobile device components using OTA	14
7.2.5	Mobile financial applications hardening techniques	14
7.2.6	Platform security services	15
7.2.7	Application level security services for mobile financial applications	16
7.2.8	Application management security services	17
7.3	Minimum set of security requirements for mobile financial services	17
7.3.1	General	17
7.3.2	Remote MFS access requirements	17
7.3.3	Transaction processing requirements	18
7.3.4	Protection of sensitive data	19
7.3.5	Mobile device requirements	20
7.3.6	Customer education	20
7.4	Minimum set of security requirements for mobile application management	21
7.4.1	Customer enrolment and provisioning requirements	21
7.4.2	Key management	21
7.4.3	Mobile financial service provider and trusted service manager exchanges	22
7.4.4	Application downloading	22
7.4.5	Application deactivation	22
7.5	Summary: Requirements for security services for mobile financial services	22
8	Security requirements for cryptographic components used for MFS	23
8.1	Mobile device secure environments	23
8.1.1	Mobile Device requirements for MFS	23
8.1.2	Software-based secure environment	24

8.1.3	Trusted execution environment (TEE)	24
8.1.4	Secure element requirements	26
8.1.5	Secure element requirements for digital signature services	28
8.2	Security requirements for cryptographic modules used for MFS	30
8.2.1	General	30
8.2.2	List of requirements for cryptographic hardware modules	30
8.2.3	Requirements for cryptographic software modules	31
9	Security evaluation and certification aspects	31
9.1	General recommendation	31
9.2	Cryptographic modules	31
9.3	Software modules	32
9.4	Interoperability of security certifications	32
9.5	Guidance for TEE security evaluation and certification	33
10	Security requirements for mobile proximate payments	33
10.1	General	33
10.2	Common security requirements	34
10.2.1	Integrity of sensitive data and applications at rest	34
10.2.2	Authentication	34
10.2.3	Data protection in transit	34
11	Security requirements for mobile remote payments	34
11.1	General	34
11.2	Security requirements	35
11.2.1	Authentication	35
11.2.2	Proof of consent	35
11.2.3	Payment gateway processing requirements	35
12	Security requirements for mobile banking	35
12.1	General	35
12.2	Authentication considerations	36
12.3	Security requirements	37
13	Electronic money	37
13.1	General	37
13.2	Anonymity requirements	37
13.3	Security requirements	37
14	Data protection requirements	38
14.1	General considerations and legal framework for compliance	38
14.2	Requirements and recommendations for data protection	39
14.2.1	Requirements	39
14.2.2	Recommendations for data protection	39
14.3	Privacy assessment	39
	Annex A (informative) Risk analysis guidelines	40
	Annex B (informative) Mobile financial system implementation of Know-Your- Customer requirements	45
	Annex C (informative) Cryptographic mechanisms for mobile financial services	46
	Annex D (informative) Vulnerabilities and attacks on mobile financial services	51
	Bibliography	55