

# ISO 11568:2023-02 (E)

## Financial services - Key management (retail)

---

<b>Contents</b>		<b>Page</b>
Foreword.....		v
Introduction.....		vi
<b>1</b>	<b>Scope</b> .....	<b>1</b>
1.1	General.....	1
1.2	Scope exclusions.....	1
<b>2</b>	<b>Normative references</b> .....	<b>1</b>
<b>3</b>	<b>Terms and definitions</b> .....	<b>2</b>
<b>4</b>	<b>Key management requirements</b> .....	<b>12</b>
4.1	General.....	12
4.1.1	Key management strategy.....	12
4.1.2	Dual control and split knowledge of secret or private keys.....	12
4.1.3	Permissible key forms.....	13
4.1.4	Logging.....	14
4.1.5	Cryptographic strength.....	15
4.1.6	Key locations.....	15
4.1.7	Single-purpose key usage.....	15
4.2	Secure cryptographic device.....	17
4.2.1	General requirements.....	17
4.2.2	Additional SCD requirements for devices used in SKDAT.....	18
4.3	Additional CA requirements.....	19
4.4	Additional RA requirements.....	19
4.5	Key blocks.....	20
4.5.1	Overview of key blocks.....	20
4.5.2	Key attributes.....	21
4.5.3	Integrity of the key block.....	21
4.5.4	Key and sensitive attributes field.....	21
4.6	Key creation.....	22
4.6.1	Symmetric key creation.....	22
4.6.2	Asymmetric key creation.....	23
4.7	Key component and key share creation.....	24
4.8	Check values.....	24
4.8.1	Introduction.....	24
4.8.2	Symmetric key check value calculation.....	25
4.8.3	Asymmetric key check value calculation.....	25
4.9	Key distribution.....	25
4.9.1	Symmetric key distribution.....	25
4.9.2	SKDAT asymmetric key distribution.....	29
4.10	Key loading.....	30
4.10.1	General.....	30
4.10.2	Loading key components or shares.....	31
4.11	Key utilization.....	32
4.11.1	General key utilization requirements.....	32
4.11.2	Additional key utilization requirements for SKDAT.....	33
4.12	Key storage.....	33
4.12.1	Cleartext key component and share storage.....	33
4.12.2	Public key storage.....	34
4.13	Key replacement.....	34
4.14	Key destruction.....	35

4.14.1	General .....	35
4.14.2	Key destruction from an SCD .....	36
4.14.3	Destruction of a key in cryptogram form .....	36
4.14.4	Component and share destruction .....	36
4.15	Key backup .....	36
4.16	Key archiving .....	36
4.17	Key compromise .....	37
<b>5</b>	<b>Transaction key management techniques .....</b>	<b>38</b>
5.1	General .....	38
5.2	Method: master keys or transaction keys .....	38
5.3	Derived unique key per transaction .....	39
5.3.1	General .....	39
5.3.2	DUKPT key management .....	39
5.3.3	Unique initial keys .....	42
5.3.4	AES DUKPT .....	43
5.3.5	KSN compatibility mode .....	46
5.3.6	Derived key OIDs .....	47
5.3.7	Keys and key sizes .....	47
5.3.8	Helper functions and definitions .....	48
5.3.9	Key derivation function algorithm .....	49
5.3.10	Derivation data .....	50
5.3.11	"Create Derivation Data" (local subroutine) .....	51
5.3.12	Security considerations .....	52
5.3.13	Host security module algorithm .....	54
5.3.14	General .....	54
5.3.15	"Derive Initial Key" .....	54
5.3.16	"Host Derive Working Key" .....	55
5.3.17	Intermediate derivation key derivation data examples .....	55
5.3.18	Working key derivation data examples .....	56
5.3.19	Transaction-originating device algorithm .....	57
5.4	Host-to-host UKPT .....	62
	<b>Annex A (informative) Key and component check values .....</b>	<b>64</b>
	<b>Annex B (normative) Split knowledge during transport .....</b>	<b>68</b>
	<b>Annex C (informative) Trust models and key establishment .....</b>	<b>70</b>
	<b>Annex D (informative) Symmetric key life cycle .....</b>	<b>78</b>
	<b>Annex E (informative) Asymmetric key life cycle phases .....</b>	<b>80</b>
	<b>Annex F (normative) Approved algorithms .....</b>	<b>83</b>
	<b>Annex G (informative) AES DUKPT pseudocode notation .....</b>	<b>84</b>
	<b>Annex H (informative) AES DUKPT test vectors .....</b>	<b>87</b>
	<b>Annex I (informative) TDEA-derived unique key per transaction .....</b>	<b>88</b>
	<b>Annex J (informative) Roles in payment environment .....</b>	<b>109</b>
	<b>Annex K (informative) Roles in symmetric key distribution using asymmetric techniques .....</b>	<b>112</b>
	<b>Bibliography .....</b>	<b>115</b>