

# ISO/IEC 18013-3:2017-04 (E)

## Information technology - Personal identification - ISO-compliant driving licence - Part 3: Access control, authentication and integrity validation

---

<b>Contents</b>		<b>Page</b>
Foreword .....		v
Introduction .....		vi
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	3
4	Abbreviated terms .....	6
5	Conformance .....	8
6	Functional requirements .....	8
6.1	Access control .....	8
6.2	Document authentication .....	8
6.3	Data integrity validation .....	8
7	Mapping of mechanisms to requirements and technologies .....	11
8	Mechanisms .....	12
8.1	Passive authentication .....	12
8.1.1	Purpose .....	12
8.1.2	Applicability .....	12
8.1.3	Description .....	12
8.1.4	Hash function .....	13
8.1.5	Signing method .....	14
8.2	Active authentication .....	17
8.2.1	Purpose .....	17
8.2.2	Applicability .....	17
8.2.3	Description .....	17
8.2.4	Mechanism .....	17
8.3	Scanning area identifier .....	19
8.3.1	Applicability .....	19
8.3.2	Description .....	19
8.4	Non-match alert .....	30
8.4.1	Purpose .....	30
8.4.2	Applicability .....	30
8.4.3	Description .....	30
8.4.4	Mechanism .....	31
8.5	Basic access protection .....	32
8.5.1	Purpose .....	32
8.5.2	Applicability .....	32
8.5.3	Description .....	32
8.5.4	Mechanism .....	33
8.6	Extended Access Control v1 .....	34
8.6.1	Purpose .....	34
8.6.2	Applicability .....	34
8.6.3	Description and mechanism .....	34
8.7	PACE .....	35

8.7.1	Purpose .....	35
8.7.2	Applicability .....	35
8.7.3	Description and mechanism .....	35
8.7.4	PACE relative to BAP .....	35
9	Security mechanism indicator .....	36
10	SIC LDS .....	37
10.1	General .....	37
10.2	EF.SOD - Document security object (short EF identifier = `1D', Tag = `77') .....	39
10.3	EF.DG12 Non-match alert (short EF identifier= `0C', Tag = `71') .....	39
10.4	EF.DG13 Active authentication (short EF identifier = `0D', Tag = `6F') .....	39
10.5	EF.DG14 EACv1 (short EF identifier = `0E', Tag = `6E') .....	40
10.6	EF.CardAccess if PACE is supported (short EF identifier = `1C') .....	40
Annex A (informative) Public key infrastructure (PKI) .....		41
Annex B (normative) Basic access protection .....		51
Annex C (normative) PACE .....		67
Annex D (normative) Extended Access Control v1 .....		72
Annex E (normative) SIC command set .....		76
Annex F (normative) List of tags used .....		78
Bibliography .....		80