

# ISO/IEC 30136:2018-03 (E)

## Information technology - Performance testing of biometric template protection schemes

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
Introduction .....		v
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	1
4	Abbreviated terms .....	3
5	Conformance .....	4
6	Methods for biometric template protection (informative) .....	4
6.1	General .....	4
6.2	Generalized architecture for biometric template protection system .....	5
6.3	Data separation .....	8
6.4	Examples of typical architectures in template protection systems .....	8
6.4.1	Biometric verification utilizing multiple databases .....	8
6.4.2	Two-factor biometric verification utilizing smart card .....	9
6.4.3	Two-factor biometric verification utilizing passwords .....	10
7	Overview of performance evaluation for biometric template protection schemes .....	10
7.1	Methods for attacking a biometric template protection system .....	10
7.2	Necessity of metrics beyond traditional recognition performance .....	10
7.3	Technology evaluation .....	11
7.4	Theoretical evaluation and empirical evaluation .....	11
7.5	Threat models .....	11
7.5.1	Naive model .....	12
7.5.2	Collision model .....	12
7.5.3	General models .....	12
8	Performance metrics for biometric template protection systems .....	13
8.1	General .....	13
8.2	Case of multiple biometric access control systems .....	13
8.3	Metrics for enrolment and verification performance .....	14
8.3.1	General .....	14
8.3.2	Accuracy degradation .....	14
8.3.3	Template diversity .....	15
8.3.4	Storage requirement per registered individual .....	16
8.4	Metrics for security and privacy protection performance .....	16
8.4.1	Irreversibility .....	16
8.4.2	Unlinkability .....	18
8.4.3	Successful Attack Rate (SAR) (optional) .....	19
Annex A (informative)	Publication of algorithms or proofs used in performance evaluations .....	21
Bibliography .....		22