

ISO/IEC 19823-11:2022-10 (E)

Information technology - Conformance test methods for security service crypto suites - Part 11: Crypto suite PRESENT-80

Contents	Page
Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Test methods	2
4.1 General.....	2
4.2 By demonstration.....	2
4.3 By design.....	2
5 Test requirements for ISO/IEC 18000-63 interrogators and tags	2
6 Test methods with respect to ISO/IEC 29167-11 interrogators and tags	2
6.1 Test map for optional features.....	2
6.2 Crypto suite requirements.....	3
6.2.1 General.....	3
6.2.2 Crypto suite requirements of ISO/IEC 29167-11, Clauses 1 to 8 and Annexes A – C.....	3
6.2.3 Crypto suite requirements of ISO/IEC 29167-11, Clauses 9 to 11 and Annex E.....	3
6.3 Test patterns.....	8
6.3.1 General.....	8
6.3.2 Test Pattern 1.....	8
6.3.3 Test Pattern 2.....	9
6.3.4 Test Pattern 3.....	9
6.3.5 Test Pattern 4.....	10
Bibliography	11