

ISO/IEC 19823-10:2017-11 (E)

Information technology - Conformance test methods for security service crypto suites - Part 10: Crypto suite AES-128

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Normative references	1
3	Terms, definitions, symbols and abbreviated terms	1
4	Test methods	2
4.1	General	2
4.2	By demonstration	2
4.3	By design	2
6.1	Test map for optional features	3
6.2	Additional parameters required as input for the test	3
6.3	Crypto suite requirements	4
6.4	Test patterns	19
Bibliography		23