ISO/IEC 27070:2021-12 (E)

Information technology - Security techniques - Requirements for establishing virtualized roots of trust

Contents

Page

Foreword ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 Symbols and abbreviated terms ... **2**

5 Functional view ... **3**
5.1 Overview ... 3
5.2 Hardware layer components ... 4
5.2.1 General ... 4
5.2.2 Functional requirements of key components ... 4
5.2.3 Security requirements of key components ... 4
5.3 VMM layer components ... 5
5.3.1 Functional requirements of key components ... 5
5.3.2 Security requirements of key components ... 6
5.4 VM layer components ... 7
5.5 Cloud OS layer components ... 8
5.5.1 General ... 8
5.5.2 Functional requirements of key components ... 8
5.5.3 Security requirements of key components ... 8

6 Activity view ... **9**
6.1 General ... 9
6.2 Transitive trust ... 9
6.2.1 General ... 9
6.2.2 Transitive trust in host ... 10
6.2.3 Transitive trust in VMM ... 10
6.2.4 Transitive trust in VM ... 10
6.3 Integrity measurement ... 10
6.4 Remote attestation ... 11
6.5 Data protection ... 12
6.5.1 General ... 12
6.5.2 Data binding ... 12
6.5.3 Data sealing ... 13
6.6 vTM migration ... 14

Annex A (informative) **Relationship between activity and functional views** ... **16**

Bibliography ... **18**