ISO/IEC 27071:2023-07 (E)

Cybersecurity - Security recommendations for establishing trusted connections between devices and services

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 1
3.1 Terms relating to cloud computing 1
3.2 Terms relating to cloud computing roles and activities 2
3.3 Terms relating to security and privacy 2
3.4 Miscellaneous terms 4

4 Abbreviated terms 5

5 Framework and components for establishing a trusted connection 5
5.1 Overview 5
5.2 Hardware security module 9
5.3 Root of trust 9
5.4 Identity 10
5.5 Authentication and key establishment 10
5.6 Remote attestation 10
5.7 Data integrity and authenticity 10
5.8 Trusted user interface 10

6 Security recommendations for establishing a trusted connection 10
6.1 Hardware security module 10
6.2 Root of trust 11
6.3 Identity 11
6.4 Authentication and key establishment 11
6.5 Remote attestation 11
6.6 Data integrity and authenticity 12
6.7 Trusted user interface 12

Annex A (informative) Threats 13

Annex B (informative) Solutions for components of a trusted connection 18

Annex C (informative) Example of establishing a trusted connection 23

Bibliography 24