ISO/IEC 20648:2024-07 (E)

Information technology - TLS specification for storage systems

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 Overview and concepts 3

5.1 General 3
5.2 Storage specifications 4
5.3 Overview of TLS 4
5.3.1 TLS background *4*
5.3.2 TLS functionality *4*
5.3.3 Summary of cipher suites *5*
5.3.4 X.509 digital certificates *6*
5.3.5 Quantum computing and TLS *7*

6 Requirements 7

6.1 TLS protocol requirements 7
6.2 Cipher suites 7
6.2.1 Required cipher suites for interoperability with TLS 1.2 ..... *7*
6.2.2 Recommended cipher suites for enhanced security with TLS 1.2 ..... *8*
6.2.3 Recommended cipher suites and extensions with TLS 1.3 ..... *9*
6.3 Digital certificates 9
6.3.1 Certificate profile requirements *9*
6.3.2 Certificate validity and path validation requirements *10*
6.3.3 Certificate encoding requirements *10*
6.4 Compression methods 10

7 Guidance for the implementation and use of TLS in data storage 11

7.1 Digital certificates 11
7.1.1 Certificate model *11*
7.1.2 Chain of trust *11*
7.1.3 Certificate lifecycle *11*
7.1.4 Revocation *11*
7.2 Security awareness 12
7.3 Cipher suites 12
7.4 Using TLS with HTTP 12
7.5 Use of pre-shared keys 12

Bibliography 14