

# ISO/IEC 20648:2016-03 (E)

## Information technology - TLS specification for storage systems

---

<b>Contents</b>		<b>Page</b>
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 .....	3
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 .....	4
5.3.4	X.509 digital certificates .....	5
6	Requirements .....	5
6.1	TLS protocol requirements .....	5
6.2	Cipher suites .....	6
6.2.1	Required cipher suites for interoperability .....	6
6.2.2	Recommended cipher suites for enhanced security .....	6
6.3	Digital certificates .....	7
7	Guidance for the implementation and use of TLS in data storage .....	7
7.1	Digital certificates .....	7
7.1.1	Certificate model .....	7
7.1.2	Chain of trust .....	8
7.1.3	Certificate lifecycle .....	8
7.1.4	Revocation .....	8
7.2	Security awareness .....	8
7.3	Cipher suites .....	9
7.4	Using TLS with HTTP .....	9
7.5	Use of pre-shared keys .....	9
Bibliography .....		11