ISO 13491-1:2024-07 (E)

Financial services - Secure cryptographic devices (retail) - Part 1: Concepts and requirements

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Abbreviated terms **4**

5 Secure cryptographic device concepts **5**
5.1 General 5
5.2 Hardware management devices 5
5.3 Secure cryptographic device types 6
5.3.1 General types 6
5.3.2 Secure cryptographic device components 6
5.3.3 Hardware security module 7
5.3.4 Key loading devices 10
5.4 Attack scenarios 10
5.4.1 General 10
5.4.2 Penetration 10
5.4.3 Monitoring 10
5.4.4 Manipulation 11
5.4.5 Modification 11
5.4.6 Substitution 11
5.5 Defence measures 11
5.5.1 General 11
5.5.2 Device characteristics 12
5.5.3 Device management 12
5.5.4 Environment 13

6 Requirements for device security characteristics **13**
6.1 General 13
6.2 Physical security requirements for secure cryptographic devices 13
6.3 Tamper-evident requirements 14
6.3.1 General 14
6.3.2 Substitution 14
6.3.3 Penetration 14
6.3.4 Modification 14
6.3.5 Monitoring 14
6.4 Tamper-resistant requirements 14
6.4.1 General 14
6.4.2 Penetration 14
6.4.3 Modification 15
6.4.4 Monitoring 15
6.4.5 Substitution or removal 15
6.5 Tamper-responsive requirements 15
6.5.1 General 15
6.5.2 Penetration 15
6.5.3 Modification 15
6.6 Logical security requirements for SCDs and HMDs 16
6.6.1 General 16
6.6.2 Dual control 16

6.6.3 Unique key per device 16
6.6.4 Assurance of genuine device 16
6.6.5 Design of functions 16
6.6.6 Use of cryptographic keys 17
6.6.7 Sensitive device states 17
6.6.8 Multiple cryptographic relationships 17
6.6.9 Secure device software authentication 17

7 Requirements for device management 17
7.1 General 17
7.2 Life cycle phases 18
7.3 Life cycle protection requirements 19
7.3.1 General 19
7.3.2 Manufacturing phase 20
7.3.3 Post-manufacturing phase 20
7.3.4 Commissioning (initial financial key loading) phase 20
7.3.5 Inactive operational phase 20
7.3.6 Active operational phase (use) 21
7.3.7 Decommissioning (post-use) phase 21
7.3.8 Repair phase 21
7.3.9 Destruction phase 22
7.4 Life cycle protection methods 22
7.4.1 Manufacturing 22
7.4.2 Post-manufacturing phase 22
7.4.3 Commissioning (initial financial key loading) phase 23
7.4.4 Inactive operational phase 23
7.4.5 Active operational (use) phase 23
7.4.6 Decommissioning phase 24
7.4.7 Repair 24
7.4.8 Destruction 24
7.5 Accountability 24
7.6 Device management principles of audit and control 25

Bibliography 27