ISO 13491-1:2007-06 (E)

Banking - Secure cryptographic devices (retail) - Part 1: Concepts, requirements and evaluation methods

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 2

4 Abbreviated terms 4

5 Secure cryptographic device concepts 4
5.1 General 4
5.2 Attack scenarios 5
5.3 Defence measures 6

6 Requirements for device security characteristics 8
6.1 Introduction 8
6.2 Physical security requirements for SCDs 8
6.3 Logical security requirements for SCDs 11

7 Requirements for device management 12
7.1 General 12
7.2 Life cycle phases 13
7.3 Life cycle protection requirements 14
7.4 Life cycle protection methods 15
7.5 Accountability 17
7.6 Device management principles of audit and control 18

8 Evaluation methods 20
8.1 General 20
8.2 Risk assessment 21
8.3 Informal evaluation method 22
8.4 Semi-formal evaluation method 24
8.5 Formal evaluation method 26

Annex A (informative) Concepts of security levels for system security 27

Bibliography 30