ISO 13133:2026-09 (E)

Financial services - Security reference model for digital currency hardware wallet (SRM-DCHW)

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Abbreviated terms 5

5 Taxonomy 7

6 Reference model of a DCHW system 8
6.1 General 8
6.2 DC life cycle 8
6.2.1 General 8
6.2.2 DC states 9
6.2.3 DC state changes 9
6.3 DCHW life cycle 10
6.3.1 General 10
6.3.2 DCHW states 10
6.3.3 DCHW state changes 10
6.4 Participants of a DCHW system 11
6.4.1 General 11
6.4.2 Issuing entities 11
6.4.3 Intermediaries 11
6.4.4 End users 11
6.4.5 TSPs 11
6.5 Conceptual model of a DCHW system 12
6.5.1 General 12
6.5.2 Issuing entity components 12
6.5.3 Intermediary components 13
6.5.4 DCHW components 13
6.5.5 Acceptance device components 13
6.6 TOE of a DCHW 14
6.6.1 General 14
6.6.2 Mobile devices 15
6.6.3 ICCs 15
6.7 TOE environment of a DCHW 15

7 Considerations for the design of a security framework 15

8 Securityproblemdefinition 16
8.1 General 16
8.2 Assets to be protected 16
8.2.1 User data 16
8.2.2 TSF hardware and software 17
8.2.3 TSF data 17
8.3 Threat actors 17

8.4 Threats ... 17
8.4.1 Threats to DC ... 17
8.4.2 Transaction threats ... 18
8.4.3 Cryptography threats ... 18
8.4.4 Communication threats ... 18
8.4.5 Authentication threats ... 19
8.4.6 User privacy threats ... 19
8.4.7 Hardware and software threats ... 19
8.4.8 Risk management threats ... 20
8.4.9 Emergency response threats ... 20

8.4.10 Monitoring threats ... 20
8.4.11 Threats to supply chain security ... 21
8.5 Organizational security policies ... 21
8.6 Assumptions ... 22

9 Security objectives ... 22
9.1 General ... 22
9.2 Security objectives for the TOE ... 22
9.2.1 DC security objectives ... 22
9.2.2 Transaction security objectives ... 23
9.2.3 Cryptography security objectives ... 24
9.2.4 Communication security objectives ... 25
9.2.5 Authentication security objectives ... 26
9.2.6 Privacy security objectives ... 26
9.2.7 Hardware and software security objectives ... 27
9.2.8 Risk management security objectives ... 28
9.2.9 Emergency response security objectives ... 28
9.2.10 Monitoring security objectives ... 28
9.2.11 Supply chain security objectives ... 29

Annex A (informative) Example models for secure implementation of DCHW on mobile devices ... 30

Annex B (informative) Examples of tiered DCHWs ... 33

Bibliography ... 34