ISO/IEC 23220-1:2023-02 (E)

Cards and security devices for personal identification - Building blocks for identity management via mobile devices - Part 1: Generic system architectures of mobile eID systems

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Abbreviated terms 6

5 Design and privacy principles of mobile document systems 7
5.1 Design principles 7
5.2 Privacy and security principles 8
5.2.1 General 8
5.2.2 Data minimization 8
5.2.3 Consent and choice: 8
5.2.4 Accuracy and quality 8
5.2.5 Information security 9

6 General life-cycle phases and components of mobile document systems 9
6.1 Life-cycle phases of mobile document systems 9
6.2 Components of a mobile document system 10
6.2.1 Operational modes of components 10
6.2.2 Components of mobile document systems 11

7 Generic system architectures of mobile document systems in installation phase 13

8 Generic system architectures of mobile document systems in issuing phase 15
8.1 Source of user attributes 15
8.2 Generic sub-phases of issuing phase 15
8.3 System architectures in sub-phases user identification and mID-discovery 16
8.4 Architectures in sub-phase issuance 18
8.5 Monitoring service in issuing phase 20

9 On-site identification system architecture in operational phase 21
9.1 General sub-phases of on-site identification system architecture 21
9.2 On-site identification system architecture with local attribute storage 21
9.3 On-site identification system architecture with remote attribute storage 22

10 Remote identification system architecture in operational phase 23
10.1 General 23
10.2 Remote identification system architecture with local attribute storage 23
10.3 Remote identification system architecture with remote attribute storage 25

Annex A (informative) Examples of deployment options for issuers in issuing phase 28

Annex B (informative) Examples of deployment options in installation phase 35

Annex C (informative) Examples of holder enrolment 39

Annex D (informative) Examples of additional physical factor(s) of authentication 43

Bibliography 47