



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 44285.1-2024

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

卡及身份识别安全设备 通过移动设备进行身份管理的构件 第1部分：移动电子身
份系统的通用系统架构

(English Translation)

Issued on: August 23, 2024

Implemented on: August 23, 2024

**Issued by: State Administration for Market Regulation, China National
Standardization Administration**

Table of Contents

Preface
Introduction
1 Scope
2 Normative references
3 Terms and Definitions
4 Abbreviations
5 Design and Privacy Principles of Mobile Credential Systems
6 Common Life Cycle Phases and Components of a Mobile Credential System
7 General system architecture of mobile ID system installation phase
8 General system architecture of the mobile certificate system issuance phase
9 On-site identification system architecture during operation phase
10 Remote ID System Architecture in Operation Phase
Appendix A (Informative) Examples of publisher deployment options during the release phase
Appendix B (Informative) Examples of Deployment Options during Installation
Appendix C (Informative) Example of holder registration
Appendix D (Informative) Examples of other physical factors for identification
References

Foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for standardization work Part 1: Structure and drafting rules for standardization documents" Drafting is required.

This document is part 1 of GB/T 44285 "Cards and identity security devices for identity management via mobile devices" GB/T 44285 has published the following parts.

--Part 1: Generic system architecture for mobile electronic identity systems.

This document is modified to adopt ISO/IEC 23220-1:2023 "Cards and identity security devices for identity management via mobile devices" Components of a mobile electronic identity system Part 1: Generic system architecture for mobile electronic identity systems.

Compared with ISO/IEC 23220-1:2023, this document has the following structural adjustments.

--3.7 "Discovery service" of this document corresponds to 3.18 of ISO/IEC 23220-1:2023.

3.8~3.18 of the document will be deferred to 3.7~3.17 of ISO/IEC 23220-1:2023 in sequence;

--B.6 of this document corresponds to the content of B.5 in ISO/IEC 23220-1:2023.

The technical differences between this document and ISO/IEC 23220-1:2023 and their reasons are as follows.

--Replace ISO/IEC 29100 and ISO/IEC 19286 with the normative references GB/T 35273 and GB/T 40660 (see 5.2.1) to adapt to my country's technical conditions and increase operability.

The following editorial changes were made to this document.

-- Added the abbreviation "TRE" (see Chapter 4);

--Added content of B.5.

Introduction

Electronic ID applications (eID applications) are usually used in badges and ID cards with integrated circuits, allowing users to complete electronic identity recognition, authentication, and Many different application areas have a fundamental need for these mechanisms and use different means to provide them.

some functions (for example, the human resources system has social security cards or medical insurance cards, the financial sector uses bank cards, and the government sector has identity cards, electronic passports or driver's licenses).

The education system has a student ID or library card, the company has an employee card, and individuals have a membership card, etc.).

Mobile devices (such as mobile phones or smartphones, wearable devices) are a core part of many people's daily lives. They are not only used for communication it is also used for sending emails, accessing social media, gaming, shopping, managing finances, and storing private content such as photos, videos, and music.

Today, they are used as personal devices for business and private applications. With the ubiquity of mobile devices in daily activities, users strongly Requires electronic identity applications (eID-Apps) or services with identity/authentication mechanisms on their mobile devices, i.e. mdoc Use the program.

An mdoc application can be deployed to provide many different digital ID credentials. In addition, it can reside on a mobile device.

In addition, users may have multiple mobile devices with mdoc applications installed, which leads to credential and enhancements to the attribute management mechanism.

The technical prerequisites for deploying mdoc applications already exist and are partially standardized to support security and Privacy. Examples of containers for eID application solutions are software-based trusted execution environments (TEEs), hardware-based secure elements, (e.g., universal integrated circuit card (UICC), embedded or integrated UICC (eUICC or iUICC), embedded secure element, secure storage card[19] or other dedicated internal secure device resident on the mobile device), and server-based security means Solution.

Since mdoc applications can be located on different forms of mobile devices with different security means, they are as universal as possible to this diversity also leads to different levels of security, trust, and assurance.

Therefore, trusted eID management means the (remote) management and use of one or several security elements (e.g. in the form of smart networks), credentials and User attributes, with different security levels appropriate to their capabilities and strengths.

The outside world accesses the mdoc application through available transmission channels. Typical local channels are 2D barcode scanning, BLE, Near Field Communication (NFC) and WLAN, etc., while long-distance communication is usually Internet connection through mobile network and WLAN network.

The selection of identification method and transmission interface and protocol is an important part of trusted eID management.

mdoc applications are used in different areas of daily life and are the focus of different standardization activities.

mechanisms and protocols to provide interoperability and interchangeability. With these basic considerations in mind, future mdoc applications can Derived from and may expand GB/T 44285.

GB/T 44285 builds on existing standards and includes four main features.

- a) Establishment of secure channel;
- b) API call serialization method;
- c) data element naming conventions;
- d) Payload transmission over the communication channel protocol.

Furthermore, it adds a means of establishing Trust on First Use (TOFU).

Note: GB/T 44285 inherits and enhances the functions adopted by the mobile driving license application, thereby ensuring backward compatibility with ISO/IEC 18013-5.

GB/T 44285 "Components of cards and identity security devices for identity management via mobile devices" is divided into the following six part.

--Part 1: Generic system architecture of mobile electronic identity system. The purpose is to determine the system generic architecture and application-related processes.

-- Part 2: Data objects and encoding rules for mobile electronic identity systems. The purpose is to determine the common data format of the system.

Easy to exchange.

--Part 3: Installation and Release Phase Protocols and Services. The purpose is to specify the release phase protocols and services.

--Part 4: Protocols and services during the operation phase. The purpose is to specify the protocols and services during the operation phase.

--Part 5: Trust model and trustworthiness assessment. The purpose is to specify the trust model and trust level.

--Part 6: Mechanisms for authenticating the trustworthiness of security zones. The purpose is to define the mechanisms for authenticating the trustworthiness of security zones.

Cards and identity security devices via mobile Building blocks for device identity management Part 1.

General system architecture of mobile electronic identity system

1 Scope

This document specifies the common system architecture and common life cycle of the infrastructure components of the mobile eID system, and also specifies the interfaces and services of the mdoc application and mobile verification application.

This document is intended for entities involved in the specification, architecture, design, testing, maintenance, administration and operation of mobile eID systems.

2 Normative references

The contents of the following documents constitute the essential clauses of this document through normative references in this document.

For referenced documents without a date, only the version corresponding to that date applies to this document; for referenced documents without a date, the latest version (including all amendments) applies to this document.

GB/T 35273 Information security technology Personal information security specification
GB/T 40660 Information security technology Basic requirements for biometric identification information protection