

ICS 35.240
CCS L64



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

GB/T 29271.3-2014

**Identification cards - Integrated circuit card programming
interfaces - Part 3: Application interface**

识别卡 集成电路卡编程接口 第3部分：应用接口

Issued on: September 3, 2014

Implemented on: February 1, 2015

**Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC**

Table of Contents

- 1 Scope
- 2 Normative references
- 3 Terms and Definitions
- 4 Abbreviations
- 5 Organizations for Interoperability

1 Scope

GB/T 29271.3-2014 is Part 3 of the Chinese series on smart card programming interfaces, and defines the application interface - the layer an application programmer actually calls. Below it sit the card, the reader and the driver, all of which differ between vendors; above it sits an application that should not have to know which. The interface therefore has to express what an application wants in terms of card services and identities rather than in terms of APDUs, while keeping the security model intact across that abstraction. The standard sets the summary and computational model, the entity relationships on the application interface, the security model, and the services and data structures the interface exposes. It took effect on 1 February 2015.

This part of GB/T 29271 defines the services supported by the client application service interface: These services respond to operation requests and operations way to express: Describe these services in a programming language-independent manner: This part is the application interface of the Open System Interconnection Reference Model defined in GB/T 9387.1-1998: it provides for customers The high-level interface of the client application, the client application uses the information storage and processing operations of the card end application as the general card interface: This section is not authorized to define concrete implementations of this interface:

2 Normative references

The following documents are essential for the application of this document: For dated references, only the dated version applies to this article pieces: For undated references, the latest edition (including all amendments) applies to this document:

GB/T 9387.1-1998 Information Technology Open System Interconnection Basic Reference Model Part 1: Basic Model (idt ISO / IEC 7498-1:1994)

GB/T 29271.1-2012 Identification Card Integrated Circuit Card Programming Interface Part 1: Architecture (ISO / IEC 24727-1: 2007, IDT)

GB/T 29271:2-2012 Identification Card Integrated Circuit Card Programming Interface Part 2: Universal Card Interface (ISO /

IEC 24727-2: 2008, IDT) ISO / IEC 7816-

11 Identification cards - Integrated circuit cards - Part 11: Authentication by biometric methods cards-Integratedcircuitcards-Part

11:Personalverificationthroughbiometricmethods) IETFRFC2141 URN Syntax May:1997

3 Terms and Definitions

The terms and definitions defined in GB/T 29271:1-2012, GB/T 29271:2-2012 and the following apply to this document: 3:1 access control list accesscontrollist A collection of access rules: 3:2 access permission accesspermission The ability to grant permission to perform an operation: 3:3 access rule accessrule The connection between the in-context operation of the card-side application and the security condition: 3:

4 Action action The operation of the card-side application required by the client application in the GB/T 29271:3 application interface: 3:5 alphacard-application Management card-side application, specific to GB/T 29271, is responsible for discovering cards and applications and providing management services: 3:6 card-application-path An ordered set of protocol endpoints that connect client applications to card-side applications in the network: 3:

7 Card application service card-application-service A collection of operations: 3:8 channel A physical channel for transferring bit information between client applications and card-side applications: 3:9 client-application client-application A software component that runs on a platform that uses data storage and computing services provided by the card-side application: 3:10 connection connection Logical reference channel: 3:11 global differential-identity Differential features identified in all card-side applications managed by the same alpha card-side application: 3:12 local differential-identity Differential features that are recognized only in the card-side application for which they are defined: 3:13 parameter parameter Information that is required to define or affect operation: 3:14 return code returncode Information, including status, is returned as a result of the operation: 3:15 securitycondition Boolean expression for the discriminative state of the difference feature: 3:16 session session Connection when used for a specific security context: 3:17 object target The entity manipulated by the operation of the card-side application service:

4 Abbreviations

The abbreviations given in GB/T 29271:1-2012, GB/T 29271:2-2012 and the following abbreviations apply to this document: ACL: Access Control List (accesscontrollist) AID: application identifier (applicationidentifier) AR: access rule (accessrule) DID: Differential-identity DSI: data structure for interoperability GCAL: generic card access layer (generic card access layer) OID: object identifier (objectidentifier) SAL: service access layer

(serviceaccesslayer)

5 Organizations for Interoperability

1 Overview The client application and the card-side application consist of two pair-level entities, which interact through well-defined transaction and communication mechanisms: The GB/T 29271:3 application interface shall be the only interface through which the client application interacts with the card-end application: This chapter defines the calculation model and permanent entity on the GB/T 29271:3 application interface, through which the client application and the card-side application communicate: interaction: The security model manages the security mechanism and establishes a trusted interaction through the security mechanism: 5:

2 Introduce the conceptual entities provided on the application interface of GB/T 29271:3, and describe their operational behaviors and relationships: 5:

3 Describe in detail the entities provided by the GB/T 29271:3 application interface and the relationships between them: 5:

4 Describe in detail the security model provided by the GB/T 29271:3 application interface: 5:

2 Computational Model 5:2:

1 The client application can identify the path to the card-side application: Using the card-side application path, the client application can initiate to the card-side application Connection: The card-side application is the card-side application currently used for connection: 5:2:2 GB/T 29271:3 application interface is a card-side application service provided to client applications: Each card-side application service consists of an operation group The operation can be requested by the client application and confirmed by the SAL return: 5:2:

3 If the client application does not know the path of the card-side application, it can request the GB/T 29271:3 application interface to find the requested card The path of the end application: 5:2:

4 Card-side applications are uniquely identified by AID: 5:2:

5 The Alpha card-side application provides the client application with the basis for the trusted management of the card-side application: 5:2:6 A client application can open multiple connections: The client application can open multiple connections to the same card-side application, and each connection is requested: Refers to a different connection handle: 5:2:

7 Using an open connection, the client application can initiate a session with the card-side application: 5:2:8 A client application can open multiple sessions: Only one session can be

opened in a connection: 5:2:

9 The current state refers to the current state of the connection defined by the current card-side application, the current data set, and the identified difference features:

Authentication state and session expressions on the connection: 5:2:

10 Card-side application includes one or more card-side application services: 5:2:

11 Specific card-side application services, named data services, provide access to zero or more data sets: 5:2:

12 The dataset contains zero or more data structures for interoperability (DSI): The dataset provides the names it contains for DSI Scope and access rules: 5:2: