ICS 35.240.15
CCS L71

中华人民共和国国家标准

GB/T XXXXX.3—202X

中华人民共和国社会保障卡一卡通规范 第3部分：安全规范

Specifications for the social security card one-card-pass of the People's Republic of China——Part 3：Security specifications

（征求意见稿）

（本草案完成时间：2023年11月04日）

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是GB/T XXXXX《中华人民共和国社会保障卡一卡通规范》的第3部分。GB/T XXXXX已经发布了以下部分：

——第1部分：基础规范；

——第2部分：应用规范；

——第3部分：安全规范；

——第4部分：终端规范。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别专利的责任。

本文件由人力资源和社会保障部提出并归口。

本文件起草单位：人力资源和社会保障部信息中心、XXX。

本文件主要起草人： XXX。

引　言

本文件通过规范社会保障卡一卡通应用实践，重点围绕社会保障卡一卡通业务需求，针对实体社会保障卡、电子社会保障卡及一卡通应用提出标准化解决方案，作为社会保障卡技术、质量管控、一卡通应用和管理要求的基础标准，对于实现社会保障卡“一卡多用、全国通用”、支撑政府公共服务一卡通、居民服务一卡通具有重要的基础指导作用并具有深远的战略意义。

GB/T XXXXX《中华人民共和国社会保障卡一卡通规范》是规范全国社会保障卡一卡通工作的基础性和通用性的标准体系，目前由4个部分构成，具体如下：

——第1部分：基础规范。目的在于规定社会保障卡一卡通的基础要求，包括社会保障卡一卡通的体系架构、载体要求、服务渠道及基础支撑要求等内容。

——第2部分：应用规范。目的在于规定社会保障卡一卡通的应用要求，包括社会保障卡一卡通的应用平台、应用场景、应用流程、应用平台接入技术要求、应用平台接入工作流程、应用协作及推广要求等内容。

——第3部分：安全规范。目的在于规定社会保障卡一卡通的安全要求，包括社会保障卡一卡通的安全体系架构、载体安全要求、终端安全要求、应用平台安全要求、数据安全要求及密钥安全要求等内容。

——第4部分：终端规范。目的在于规定社会保障卡一卡通的终端要求，包括社会保障卡一卡通的终端形态、终端通用要求、终端技术要求等内容。

中华人民共和国社会保障卡一卡通规范
第3部分：安全规范

1 范围

本文件规定了社会保障卡一卡通的安全体系架构、载体安全要求、终端安全要求、应用平台安全要求、数据安全要求及密钥安全要求。

本文件适用于社会保障卡一卡通的体系设计、开发、集成、应用、维护及运营等。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 16649.4 识别卡 集成电路卡 第4部分：用于交换的结构、安全和命令

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25069 信息安全技术 术语

GB/T 29246 信息技术 安全技术信息安全管理体系 概述和词汇

GB/T 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32907 信息安全技术 SM4 分组密码算法

GB/T 32918.4 信息安全技术 SM2 椭圆曲线公钥密码算法 第4部分:公钥加密算法

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 37092 信息安全技术 密码模块安全要求

GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

GB/T 38542 信息安全技术 基于生物特征识别的移动智能终端身份鉴别技术框架

GB/T 39204 信息安全技术 关键信息基础设施安全保护要求

GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

GB/T 40660—2021 信息安全技术 生物特征识别信息保护基本要求

GB/T 41479—2022 信息安全技术 网络数据处理安全要求

GB/T 41803.1 信息技术 社会保障卡生物特征识别应用系统 第1部分：通用要求

GB/T 41819—2022 信息安全技术 人脸识别数据安全要求

GB/T XXXXX.4—202X 中华人民共和国社会保障卡一卡通规范 第4部分：终端规范

LD/T 02—2022（所有部分） 人力资源社会保障电子认证体系规范

LD/T 03—2022 人力资源社会保障电子认证服务管理规范

LD/T 33—2015 社会保障卡读写终端规范

3 术语和定义

GB/T 25069、GB/T 29246界定的以及下列术语和定义适用于本文件。

3.1

数据安全 data security

通过管理和技术措施，确保数据有效保护和合规使用的状态。

3.2

密钥 key

控制密码变换操作的符号序列。

[来源：GB/T 25069—2022，3.389]

3.3

电子社会保障卡服务渠道 electronic social security card service channel

申请接入全国社会保障卡服务平台、对外提供电子社会保障卡签发和应用服务的载体。具体形式有APP、公众号、生活号、小程序等。

3.4

密码算法 cryptographic algorithm

描述密码处理过程的算法。

[来源：GB/T 25069—2022，3.380]

3.5

加密 encrypt

对数据进行密码变换以产生密文的过程。

[来源：GB/T 25069—2022，3.278]

3.6

解密 decrypt

加密过程对应的逆过程。

[来源：GB/T 25069—2022，3.305]

3.7

敏感数据 sensitive data

需防止被非法泄露、修改或破坏的数据。包括：姓名、社会保障号码（公民身份号码）、手机号码、地址、银行卡号、电子社会保障卡卡号、电子社会保障卡密码、签发号、生物特征信息（如人脸相片等）、征信信息、交易信息等。

3.8

明文 plain text

未加密的信息。

[来源：GB/T 25069—2022，3.425]

3.9

保密性 confidentiality

信息对未授权的个人、实体或过程不可用或不泄露的性质。

[来源：GB/T 25069—2022，3.41]

3.10

完整性 integrity

准确和完备的性质。

[来源：GB/T 25069—2022，3.612]

3.11

公钥 public key

非对称密码算法中可公开的密钥。

[来源：GB/T 25069—2022，3.211]

3.12

攻击 attack

企图破坏、泄露、篡改、损伤、窃取、未授权访问或未授权使用资产的行为。

[来源：GB/T 29246—2017，2.3]

3.13

数字签名 digital signature

附加在数据单元上的一些数据，或是对数据单元做密码变换，这种附加数据或密码变换被数据单元的接收者用以确认数据单元的来源和完整性，达到保护数据，防止被人（例如接收者）伪造的目的。

[来源：GB/T 25069—2022，3.576]

3.14

安全存取模块 secure access module

一种能够提供必要的安全机制以防止外界对终端所储存或处理的数据进行非法攻击的硬件加密模块。

3.15

电子认证 electronic authentication

采用电子技术检验用户真实性的操作。

3.16

可用性 availability

可由经授权实体按需访问和使用的性质。

[来源：GB/T 25069—2022，3.345]

3.17

SQL 注入 sql lnjection

利用程序漏洞攻击数据库服务器的方法。

3.18

密文 cipher text

采用密码算法，经过变换将其信息内容隐藏起来的数据。

[来源：GB/T 25069—2022，3.388]

3.19

数字证书 digital certificate

由国家认可的，具有权威性、可信性和公正性的第三方证书认证机构（CA）进行数字签名的一个可信的数字化文件。

[来源：GB/T 25069—2022，3.579]

3.20

私钥 private key

非对称密钥密码算法中只能由拥有者使用的不公开密钥。

[来源：GB/T 25069—2022，3.580]

3.21

数据处理 data processing

对原始数据进行抽取、转换、加载的过程。

3.22

数据脱敏 data desensilization

通过一系列数据处理方法对原始数据进行处理以屏蔽敏感数据的一种数据保护方法。

3.23

合规 compliance

对信息安全所适用的法律法规的符合程度。

3.24

加壳 packing

利用压缩、加密等技术保护文件的手段。

3.25

代码混淆 code obfuscation

将计算机程序的代码转换成一种功能上等价，却难于阅读和理解的形式的行为。

3.26

对称密钥 symmetric key

对称密码算法的密钥。

[来源：GB/T 25069—2022，3.135]

3.27

非对称密钥对 asymmetric key pair

非对称密钥

非对称密码算法中相关联的公钥和私钥。

[来源：GB/T 25069—2022，3.151]

4 缩略语

下列缩略语适用于本文件。

AK：电子社会保障卡服务渠道网关认证身份密钥（Access Key）
APDU：应用协议数据单元（Application Protocol Data Unit）
API：应用程序编程接口（Application Programming Interface）
APP：应用程序（Application）
CA：证书认证机构（Certification Authority）
CLA：命令报文的类别字节（Class Byte of the Command Message）
DDoS：分布式拒绝服务（Distributed Denial of Service）
DK：电子社会保障卡服务渠道数据加密密钥（Digital Key）
HTML5：超文本标记语言5.0（Hypertext Markup Language 5.0）
INS：命令报文的指令字节（Instruction Byte of Command Message）
IP：互联网协议（Internet Protocol）
IPv4：互联网协议第4版（Internet Protocol Version 4）
IPv6：互联网协议第6版（Internet Protocol Version 6）
Lc：终端发出的命令数据的实际长度（exact Length of data sent by the TAL in a case 3 or 4 command）
MAC：报文鉴别代码（Message Authentication Code）
PIN：个人密码（Personal Identification Number）
PSAM：服务网点终端安全存取模块（Point of service Security Access Module）
RA：证书注册机构（Registration Authority）
SDK：软件开发工具包（Software Development Kit）
SK：电子社会保障卡服务渠道网关签名验签密钥（Security Key）
SM2：椭圆曲线公钥密码算法（public key cryptographic algorithm SM2 based on elliptic curves）
SM3：密码杂凑算法（SM3 cryptographic hash algorithm）
SM4：分组密码算法（SM4 block cipher algorithm）
SSH：安全外壳协议（Secure Shell）
SSL：安全套接层（Secure Sockets Layer）
TLS：传输层安全性协议（Transport Layer Security）
URI： 统一资源标识符（Uniform Resource Identifier)
USB：通用串行总线（Universal Serial Bus）
VPN：虚拟专用网络（Virtual Private Network）

5 一卡通安全体系架构

社会保障卡一卡通安全体系架构分为五个部分，包括一卡通载体安全、一卡通终端安全、一卡通应用平台安全、一卡通数据安全、一卡通密钥安全，总体架构如图1所示。

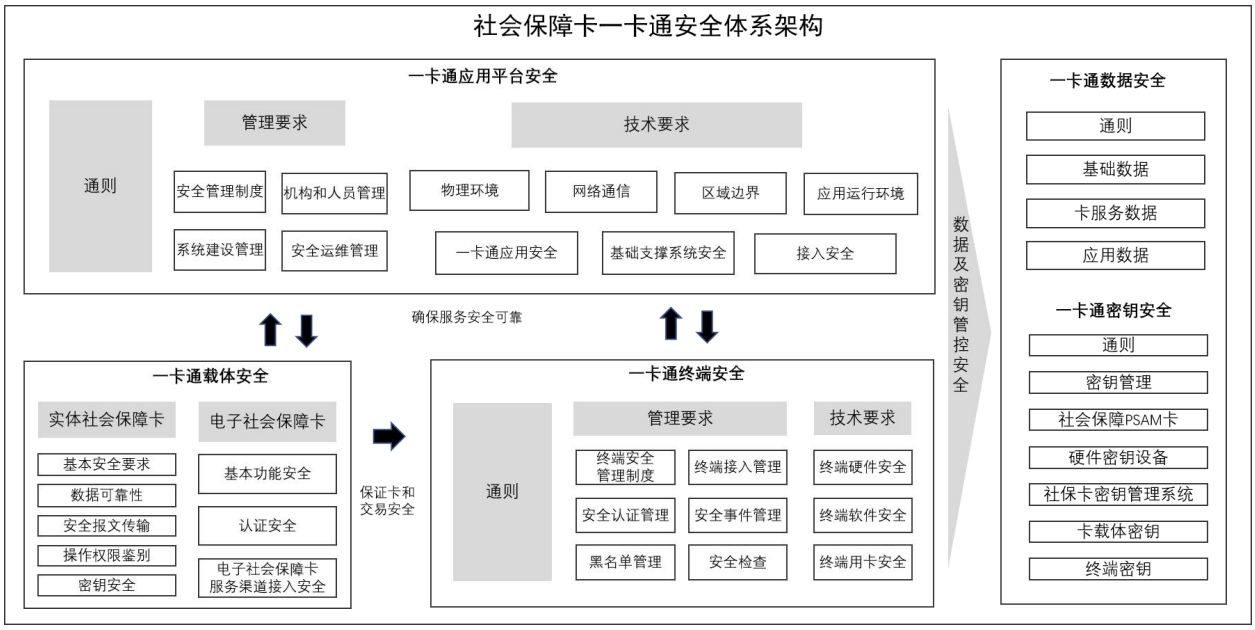

图1 社会保障卡一卡通安全体系架构

具体说明如下：

a) 一卡通载体安全：一卡通载体是持卡人同应用进行交互的介质，从卡本身安全及持卡人使用卡过程考虑安全性。一卡通载体主要包括实体社会保障卡和电子社会保障卡，实体社会保障卡安全包括基本安全要求、数据可靠性、安全报文传输、操作权限鉴别、密钥安全等；电子社会保障卡安全包括基本功能安全、认证安全、电子社会保障卡服务渠道接入安全等。

b) 一卡通终端安全：一卡通终端是能够操作一卡通载体，用于各项一卡通应用场景业务办理中并完成一定事务的设备。主要包括管理和技术两方面要求，管理方面分为终端安全管理制度、终端接入管理、安全认证管理、安全事件管理、黑名单管理、安全检查等；技术方面分为终端硬件安全、终端软件安全、终端用卡安全等。

c) 一卡通应用平台安全：一卡通应用平台是一卡通安全体系的核心部分，具备一卡通服务能力及管理功能，实现一卡通数据的安全存储处理和平台稳定可靠运行。主要包括管理和技术两方面要求。管理方面分为安全管理制度、机构和人员管理、系统建设管理、安全运维管理等；技术方面分为物理环境、网络通信、区域边界、应用运行环境、一卡通应用安全、基础支撑系统安全和接入安全等。

d) 一卡通数据安全：指一卡通应用平台在提供服务过程中，各级人力资源和社会保障部门及相关主体对一卡通数据进行收集、传输、存储、加工和使用、提供、公开、销毁等整个过程中的安全防护。

e) 一卡通密钥安全：主要包括密钥管理、社会保障 PSAM 卡管理、硬件密钥设备安全、社会保障卡密钥管理系统安全、卡载体密钥安全、终端密钥安全等。

6 一卡通载体安全要求

6.1 实体社会保障卡安全

6.1.1 基本安全要求

6.1.1.1 共存应用

各应用应通过卡内操作系统内部防火墙机制，从安全、文件系统、命令等方面确保独立管理，保障应用安全。各应用不应与个性化要求以及卡内共存的其他应用规则发生冲突。

6.1.1.2 安全计算的操作环境

与密钥有关的所有计算过程（包括密钥的产生、派生、传输、鉴别等）应在保密、安全和可靠的环境中进行。这种环境应由已采取相关措施的物理空间提供。

6.1.1.3 密码算法的安全要求

实体社会保障卡中所存储的实现密码算法的代码模块，在卡的整个生命周期中不能被修改，也不能被读取、泄露至卡外部。

6.1.1.4 PIN 的安全要求

实体社会保障卡应保证PIN在其中安全存放，且在任何情况下都不会被泄露。通过PIN进行校验时可尝试次数为6次。对于涉及敏感数据功能操作或者业务申办操作，应考虑重新进行PIN校验。

6.1.2 数据可靠性

数据可靠性应符合以下要求：

a) 为保证命令中明文数据的保密性，可将数据加密。所使用的数据加密技术应符合命令发送方和当前实体社会保障卡中被选择的应用的共同约定；
b) 当命令中要求的明文数据需要加密时，应首先格式化为以下形式的数据块：
   1） 明文数据的长度，不包括填充字符；
   2） 明文数据；
   3） 填充字符（符合附录 A.5、A.6 的要求）；
c) 格式化后的数据块应使用 A.5 描述的数据加密技术进行加密；
d) 实体社会保障卡接收命令后，应对命令中的加密数据进行解密。解密方法符合附录 A.6 的要求。

6.1.3 安全报文传输

安全报文传输应符合以下要求：

a) 安全报文传送的目的是保证数据的保密性、完整性和对发送方的认证。数据的保密性通过对数据域的加密来保证。数据的完整性和对发送方的认证通过使用 MAC 来实现；
b) 数据加密和 MAC 计算使用的过程密钥由相应功能的原始密钥和随机数产生，产生后只能在当前过程中使用一次；
c) 安全报文传送格式应符合 GB/T 16649.4 的规定。MAC 计算方法符合附录 A.1、A.2 的要求。

6.1.4 操作权限鉴别

卡内敏感数据读写应使用操作权限鉴别验证其操作合法性。鉴别数据由鉴别过程密钥对原始数据进行加密产生，操作权限鉴别过程中用到的过程密钥由鉴别命令的原始密钥和引用的可变数据（如随机数）产生，且过程密钥产生后只能在鉴别过程中使用一次。过程密钥的计算方法符合附录A.3的要求，鉴别数据的计算方法符合附录A.4的要求。

6.1.5 密钥安全

密钥管理对于保证密钥全生命周期的安全性至关重要，可以保证密钥（除公钥外）不被非授权的访问、使用、泄露、修改和替换，可以保证公钥不被非授权的修改和替换。

实体社会保障卡作为一卡通体系的线下载体，提供基础的安全支撑。一卡通密钥体系需要符合密钥管理、社会保障PSAM卡管理、硬件密钥设备安全、密钥管理系统安全、卡载体密钥安全、终端密钥安全等方面的安全要求。这些要求包括但不限于安全的密码算法、密钥全生命周期的安全性、PSAM卡的认证和监管、硬件密钥设备的保管和检查、密钥管理系统的使用、卡内密钥的独立性、一卡通终端密钥的生命周期管理等。具体要求见第10章。

为了确保实体社会保障卡密钥的安全性，应从以下方面进行防护：

a) 在密钥的装载和更新过程中使用安全报文传输，并进行加密；
b) 实体社会保障卡应具备全生命周期管理功能，以防止失效或过期密钥的使用，并保护卡内存储的密钥免受外部攻击泄露的影响；
c) 密钥管理采用按类分级管理方式，具体内容符合附录 A.7 的要求。

6.2 电子社会保障卡安全

6.2.1 基本功能安全

6.2.1.1 用户注册

在用户注册客户端环节应提供有效的用户注册机制，采用安全的用户注册方式，实现用户实名制。

6.2.1.2 登录功能

登录功能设置应符合以下要求：

a) 不应单独使用手机号码加短信验证码方式进行登录，可选择使用电子社会保障卡授权、登录密码、人脸识别（手机设备）、指纹密码（手机设备）、手势密码等方式登录。其中，人脸识别（手机设备）、指纹密码（手机设备）、手势密码应由用户主动开通，不应默认开启；
b) 除业务规则有特殊规定外应在新设备登录、敏感数据修改、支付交易、密码修改或重置时，提供双因素鉴别机制；
c) 登录状态不应长期有效，超过一定期限（最长 72h）应强制用户重新登录。

6.2.1.3 信息展示

信息展示应符合以下要求：

a) 应提供安全输入控件用于敏感数据的输入，在敏感数据输入时应进行屏蔽处理，不应截屏、录屏；
b) 姓名、社会保障号码、社会保障卡卡号、银行卡号、手机号码、地址等敏感数据的展示，应进行屏蔽处理。如需展示完整信息，应通过身份校验认证后方可展示；
c) 电子社会保障卡的条码显示时间超过一定期限（60s）应强制刷新。

6.2.1.4 身份验证

用户身份验证应符合以下要求：

a) 用户在使用电子社会保障卡功能时，如涉及敏感数据功能操作或者业务申办操作，应重新调用电子社会保障卡相关身份验证接口，不应使用客户端缓存或者使用其他方式进行身份验证；
b) 在远程服务场景下（即无面对面人工检查），采用人脸识别方式验证身份时应进行活体检测；
c) 基于人脸识别技术的活体检测功能应通过摄像头对人脸信息进行采集，应采用有效的技术手段防止摄像头在采集信息时被禁用、绕过或者替换；
d) 应确保视频、音频的输入来自实时采集的设备终端，不应使用提前录制好的视频、音频；
e) 人脸比对所用相片应从活体检测视频流中随机取帧，不应使用提前存储的相片。

6.2.1.5 用户退出

用户登录后，长时间不操作或者主动退出，当前用户登录不再有效，应拒绝用户进入电子社会保障卡进行相关功能操作。

6.2.2 认证安全

6.2.2.1 生物特征识别

生物特征识别使用应遵循GB/T 38542的相关要求。

6.2.2.2 图形验证码

图形验证码应具有使用时间限制并仅能使用一次。图形验证码应由服务器生成，客户端源文件中不应包含图形验证码文本内容。图形验证码不应作为独立的身份验证要素。

6.2.2.3 短信验证码

短信验证码应符合以下要求：

a) 短信验证码应仅可使用一次，且仅限于在规定时间内使用。短信验证码应具备长度和随机性的要求。包含短信验证码的短信内容中，应告知用户短信验证码的用途；
b) 对于采用短信验证码的客户端，应建立手机号码的谨慎变更机制，如：手机号码通过线上变更时进行额外的身份认证操作，并进行一定次数限制（如 72h 内最多一次通过线上变更手机号码）。

6.2.2.4 手势密码

手势密码应至少设置连续不间断的4个点。若手势密码存储在客户端本地，应加密存储。

6.2.2.5 口令安全

口令安全应符合以下要求：

a) 应提供口令复杂度校验功能，保证用户设置的口令达到一定的强度，避免采用简单口令（如有规律的数字）或与用户个人信息相似度过高的口令（如：生日信息、社会保障号码或者卡号的某段信息）；
b) 应在用户重置口令时，通过双因素认证机制进行额外的身份认证操作以确认用户身份；
c) 应在用户首次登录时提示用户对初始口令进行修改。

6.2.2.6 二维码安全

二维码安全应符合以下要求：

a) 应对登录二维码的真实性、有效性进行验证；
b) 应采用数字签名等密码技术生成付款二维码。二维码应具备防篡改、防重放能力。

6.2.2.7 认证失败处理

应对密码验证、生物特征识别、短信验证、手势密码等用户无效验证次数进行限制，合理设定失败次数上限（如24h内不应超过6次）和累计失败次数上限。对超过验证次数限制的账号采取合理措施进行控制。

6.2.3 电子社会保障卡服务渠道接入安全

6.2.3.1 管理安全

电子社会保障卡服务渠道接入管理应符合以下要求：

a) 电子社会保障卡服务渠道接入方首次申请接入时应提供专业机构出具的安全检测报告；
b) 电子社会保障卡服务渠道接入方应在符合电子社会保障卡服务渠道管理要求的基础上建立安全管理办法，明确电子社会保障卡服务渠道接入主要负责人、配备专人管理与对接人员，负责接入管理、运行管理、安全管理等方面；
c) 电子社会保障卡服务渠道接入方应根据不同的管理范围制定完善的审批以及应急处置方案；
d) 电子社会保障卡服务渠道接入方应每年对安全管理办法进行复查，并根据实际情况对版本进行修订；
e) 在安全检测有效期满、电子社会保障卡服务渠道系统（客户端）有重大升级或者安全策略重大调整时，电子社会保障卡服务渠道接入方应再次进行安全检测，并提交安全检测报告。

6.2.3.2 电子社会保障卡服务渠道系统（客户端）安全

6.2.3.2.1 基本功能安全

电子社会保障卡服务渠道系统（客户端）基本功能安全应符合6.2.1的要求。

6.2.3.2.2 电子社会保障卡服务渠道安全

电子社会保障卡服务渠道安全应符合附录B.2的要求。

6.2.3.2.3 认证安全

电子社会保障卡服务渠道系统（客户端）认证安全应符合6.2.2的要求。

6.2.3.2.4 数据安全

电子社会保障卡服务渠道接入方应对电子社会保障卡服务渠道系统（客户端）中数据在输入、传输、使用、存储、删除过程中进行有效安全防护，应符合附录B.3的要求。

6.2.3.2.5 通信安全

电子社会保障卡服务渠道系统（客户端）通信安全应符合附录B.4的要求。

6.2.3.2.6 接口安全

电子社会保障卡服务渠道系统（客户端）接口应符合以下要求：

a) 应对接口进行安全保护，校验调用方的接口访问权限，防止其他应用对接口进行非授权调用，见附录 B.6；
b) 对于接口的访问应基于密码技术进行有效身份鉴别，确保接口调用方身份的真实性；
c) 身份认证技术应具备抗重放攻击的能力。

6.2.3.2.7 密码算法安全

电子社会保障卡服务渠道系统（客户端）使用的密码算法应符合以下要求：

a) 渠道服务端系统使用对称密码算法、非对称密码算法和密码杂凑算法实现有关密码服务各项功能，符合附录 B.5 的要求；
b) 应采用国家有关主管部门批准的密码算法，密码算法和密码操作应由硬件或受保护的软件支撑实现。

6.2.3.2.8 密钥安全

电子社会保障卡服务渠道系统（客户端）应对使用的密钥进行全生命周期管理，包括密钥生成、交换、存取、分配、销毁等环节，符合附录B.7的要求。

6.2.3.2.9 应用安全

应用安全应符合以下要求：

a) 对于电子社会保障卡服务渠道系统（客户端）的应用安全管理，应采取安全措施确保软件自身的安全性，包括但不限于开展安全漏洞扫描、病毒查杀等；
b) 应符合附录 B.8、B.9 的要求。

7 一卡通终端安全要求

7.1 通则

一卡通终端出厂时应保证终端唯一识别码的唯一性，应符合GB/T XXXXX.4—202X中7.5.2中的要求，并通过国家或者行业认可的第三方检测机构的检测。

7.2 管理要求

7.2.1 终端安全管理制度

安全管理制度应符合以下要求：

a) 各单位应结合实际情况制定终端安全管理制度，实现对一卡通终端全生命周期的安全管理；
b) 终端安全管理制度中应涵盖人员、资产、流程等方面的内容；
c) 终端安全管理制度中应涵盖新增、注销、变更、登记、备案等方面的要求。

7.2.2 终端接入管理

应对一卡通终端接入的计算机运行环境进行安全检测，确保接入计算机的安全可信。

7.2.3 安全认证管理

应建立一卡通终端管理台账，在一卡通终端使用过程中应对终端唯一识别码、使用机构、一卡通终端权限、一卡通终端状态（如正常、丢失、损坏、注销等）进行核对，确保一卡通终端的合法使用。

7.2.4 安全事件管理

安全事件管理应符合以下要求：

a) 应建立终端损坏、丢失、盗用等安全事件报告和事件响应机制，并制定事件响应报告及响应流程、事件相关人员职责及处置权限；
b) 应记录安全事件发生情况、所采取的措施、处理结果等内容；
c) 对于发生的安全事件要进行原因分析、响应方案评估、责任认定。

7.2.5 黑名单管理

黑名单管理应符合以下要求：

a) 黑名单管理机制：应建立对一卡通终端的黑名单管理机制，实现对一卡通终端黑名单的安全管理，主要涉及黑名单的记录格式、检索和更新；
b) 黑名单的记录格式：黑名单应能按照统一的数据格式对一卡通终端唯一识别码、一卡通终端使用机构、一卡通终端权限等内容进行记录；
c) 黑名单的检索：黑名单应依据所记录的内容、格式提供相应的检索功能；

d) 黑名单的同步和更新：应在安全环境下进行，操作过程中应确保黑名单数据的安全性与完整性。

7.2.6 安全检查

应定期对一卡通终端进行安全检查，并保存安全检查结果记录。

7.3 技术要求

7.3.1 终端硬件安全

7.3.1.1 安全存取模块安全

7.3.1.1.1 安全存取模块物理安全

安全存取模块物理安全应符合LD/T 33—2015 的相关要求。

7.3.1.1.2 安全存取模块逻辑安全

安全存取模块逻辑安全应符合LD/T 33—2015 的相关要求。

7.3.1.1.3 安全存储模块计算要求

安全存取模块应支持密钥分散计算、数据加密计算、安全报文加密计算等安全计算方法，安全计算方法应采用国家有关主管部门批准的密码算法，推荐优先采用国产密码算法。

7.3.1.2 密码键盘安全要求

密码键盘安全应符合以下要求：

a） 密码键盘应实现隐私保护和防窥功能；

b） 在 PIN 输入过程中，一卡通终端应对输入的 PIN 信息进行安全遮蔽，避免通过视觉或者听觉的反馈方式泄露；

c） 对于有显示屏的密码键盘，应以不泄漏 PIN 的方式显示每一个输入的数字，比如以*号代替数字显示；

d） 在 PIN 输入过程中发生以下任意一种情况后，应自动清除内部缓存：

1） 在交易结束后；

2） 在超时的情况下（包括在一个 PIN 字符输入后过去很长时间的情况）。

7.3.2 终端软件安全

7.3.2.1 代码安全要求

代码安全应符合以下要求：

a） 终端软件应能提供安全保护机制防范恶意代码攻击；

b） 应能检测识别非授权访问、权限异常变化、恶意软件安装等行为，并采取相应安全措施（如拒绝访问、数据隔离等），确保防止恶意代码攻击、逆向分析终端软件等安全事件的发生。

7.3.2.2 算法安全要求

应使用对称加密算法、非对称加密算法和密码杂凑算法对交易敏感信息（包括支付交易中的认证信息、交互信息和敏感信息）进行加密保护。

7.3.2.3 存储安全要求

通用数据应存放在存储器中。在更新参数以及下载新的应用程序时，一卡通终端应执行以下操作：

a) 验证更新方的身份；

b) 校验下载参数及应用程序的完整性；
c) 在任何情况下，终端的应用数据均不会随意改变或丢失，并保证数据有效。

7.3.2.4 交互安全要求

交互安全应符合以下要求：

a） 应对一卡通终端接口交互过程中传输的敏感信息采用密码算法进行加密保护，保证该传输数据在被截取后无法获得明文，达到传输的保密性要求；
b） 应对一卡通终端接口交互过程中传输的敏感信息采用密码算法进行校验计算，以发现信息被篡改、删除和插入等情况，达到传输过程中的信息完整性要求。

7.3.2.5 安全日志要求

一卡通终端应能够将全部操作行为同步至接入的计算机中并形成安全日志。日志内容至少包括主体文件、操作时间、操作内容等。

7.3.2.6 漏洞检测要求

对于终端软件的研发、测试与发布，应进行阶段性的安全漏洞扫描，确保软件自身的安全性。

7.3.2.7 病毒查杀要求

对于终端软件的研发、测试与发布，应进行阶段性的程序病毒查杀，确保软件自身的安全性。

7.3.3 终端用卡安全

7.3.3.1 实体社会保障卡用卡安全

实体社会保障卡使用前应优先对卡片进行内部认证操作，确保卡片的真实性和有效性；并确保终端使用过程中所执行的APDU指令与卡数据不被窃取或篡改。

7.3.3.2 电子社会保障卡扫码认证安全

电子社会保障卡扫码认证应符合行业主管部门关于电子社会保障卡扫码认证、实人认证、登录认证以及移动支付等业务流程的相关要求。具体要求如下：

a） 获取电子社会保障卡二维码数据过程中，应确保二维码数据的完整性；
b） 获取电子社会保障卡二维码数据过程中，应根据电子社会保障卡二维码生成规则对获取到的二维码数据进行校验；
c） 电子社会保障卡二维码认证应符合 6.2.2.6 a）的要求；
d） 电子社会保障卡二维码认证过程中，应对返回的用户信息进行加密处理，确保用户信息的安全保密性。

8 一卡通应用平台安全要求

8.1 通则

本章节从管理和技术两个层面规定了一卡通应用平台安全要求，保障社会保障卡一卡通办事凭证、支付结算、待遇发放等应用能力的稳定输出。

一卡通应用平台包括一卡通应用及其基础支撑系统。基础支撑系统包括社会保障卡管理信息系统、社会保障卡持卡人员基础信息库、全国社会保障卡服务平台、电子认证系统、社会保障卡密钥管理系统等。一卡通应用平台应至少符合GB/T 22239 网络安全等级保护第三级安全防护要求。

8.2 管理要求

8.2.1 管理制度

管理制度方面应符合以下要求：

a） 应定期对安全管理制度、密码应用管理制度和操作规程的合理性和适用性进行论证和审定，对存在的不足或者需要改进之处进行修订；

b） 管理制度和操作规程应覆盖一卡通应用、社会保障卡管理信息系统、社会保障卡持卡人员基础信息库、全国社会保障卡服务平台、电子认证系统、社会保障卡密钥管理等系统。

8.2.2 机构和人员

8.2.2.1 管理机构

管理机构方面应符合以下要求：

a） 人力资源和社会保障部应设立网络安全和信息化工作领导小组，统筹指导和管理国家及地方一卡通应用平台网络安全工作，各级人力资源和社会保障部门应成立各自领导小组，承担平台网络安全工作领导职责；

b） 应设立系统管理员、安全管理员、审计管理员、密钥管理员和业务操作员等岗位，由专人担任，安全管理员、审计管理员不应兼任其他角色。

8.2.2.2 人员管理

8.2.2.2.1 工作人员管理

工作人员管理方面应符合以下要求：

a） 应建立岗位责任制度，明确各岗位在平台管理中的职责和权限；

b） 应对系统管理员、安全管理员、审计管理员、密钥管理员和业务操作员等岗位制定培训计划，培训内容应涉及安全操作、运行维护和安全管理方面；

c） 应定期对各岗位人员进行培训及考核，并告知相关的安全责任和惩戒措施；

d） 如因人员岗位变动等需分配、变更账号或权限，应由其所在部门明确账号或权限分配、变更需求，经审批通过后统一配置；

e） 应建立应用系统账户的授权审批流程，按照“最小授权、权限分离、任期有限”的原则对应用系统各类岗位进行权限划分，各岗位间的权限应保持相互独立、相互制约、相互监督；

f） 因工作需要，对超出授权范围的临时性授权应严格按照最小原则，并建立临时性授权的控制程序文件，实行事前控制、事中监督和事后审计，做好操作记录；

g） 工作人员调离岗位后，应按规定移交全部资料文档，及时注销其账户或更换其账户口令，并做好相关记录。

8.2.2.2.2 第三方人员管理

第三方人员管理方面应符合以下要求：

a) 应与第三方人员签署保密协议，不应泄露保密信息或敏感信息；

b) 第三方人员进入安全区域前应先提出书面申请，批准后由专人全程陪同，并登记备案；

c) 第三方人员访问受控网络、操作重要的主机和设备前应先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；

d) 应对第三方人员的操作进行全程监控和审计；

e) 第三方人员工作结束后应及时清除其所有的账户及访问权限。

8.2.3 系统建设管理

8.2.3.1 方案设计

一卡通应用平台的安全规划和建设方案应通过相关部门和有关安全专家的论证和审定，并经过一卡通应用平台管理部门批准后实施。

8.2.3.2 开发建设

开发建设方面应符合以下要求：

a） 应严格按照代码安全相关制度的要求进行开发；

b） 应做好对一卡通应用平台开发环境的安全管理，开发环境要相对独立，开发环境、测试环境与生产环境进行分离，不应通过开发环境直接访问生产环境服务区；

c） 应对系统程序、源代码、文档等相关资料登记造册，并设专人保管；重要文档不应通过互联网传输、不应发布到互联网；

d） 应规范版本控制和管理，定义应用系统程序和源代码的版本号编码规则，版本变更应登记时间、版本号和变更内容；

e） 应采购和使用符合国家有关规定的产品，产品类型包括但不限于网络安全产品、密码设备、终端、服务器和存储等。

8.2.3.3 系统交付

系统交付方面应符合以下要求：

a） 在交付前应进行验收测评，测评内容包括功能测试、性能测试、安全测试等，并根据测评结果完成整改，其中功能测试应至少涵盖系统的重要指标，安全测试内容应包括代码安全审计、渗透性测试、漏洞扫描等方面；各项测评完成后均需出具测试人员确认的测试报告；

b） 应制定交付清单，清单中应包括应用系统程序、源代码、文档等相关资料，并根据交付清单对所交接的设备、软件和文档进行清点。

8.2.4 安全运维管理

8.2.4.1 运维终端安全

运维终端安全方面应符合以下要求：

a） 应按照安全管理制度要求采取安全防护措施，包括统一部署终端杀毒软件、终端管控软件等，及时识别安全漏洞和隐患并进行修补；

b） 应定期检查违反规定上网（有线或者无线方式），或者其他违反安全策略的行为；

c） 应严格限制运维终端连接手机、相机、移动存储设备等存储介质。

8.2.4.2 资产管理

资产管理方面应符合以下要求：

a）一卡通应用平台服务器部署在人力资源和社会保障部门自建的机房内并组织管理的，由一卡通应用平台运营单位负责资产管理和安全管理，并保留维护记录；

b）一卡通应用平台服务器委托专业的运营机构管理的，受托机构应负责基础设施的安全，一卡通应用平台运营单位负责对一卡通应用平台各种软件和网络等进行资产管理和安全管理，并保留维护记录及委托服务协议；

c）一卡通应用平台服务器应建立资产清单，应放置在通风良好、温度适宜、防尘防潮等安全的环境内。

8.2.4.3 安全操作和维护

安全操作和维护方面应符合以下要求：

a） 应制定防护设备安全策略，并指定专人定期进行安全事件分析和安全策略配置优化；在变更防护设备配置规则之前，确保变更已进行验证和审批；

b） 应通过定期巡检、实时监测、异常处理和问题收集等多种方式确保应用系统运行安全；
c） 运行维护应进行详细的工作记录，包括维护时间、维护内容和维护人员等信息；
d） 应定期组织开展安全测评，对影响系统安全的各种因素进行评估，分析安全措施的有效性，提出漏洞修补方案并督促整改；
e） 在一卡通应用平台遭到入侵、管理员轮换、口令泄露及其他可能威胁口令安全的情况下，应及时修改口令；
f） 应确保第三方软件和组件许可信息持续有效；
g） 一卡通应用平台升级发布前，应由一卡通应用平台管理部门针对涉及变更的部分进行安全检查。

8.2.4.4 系统容灾备份

系统容灾备份方面应符合以下要求：
a） 应提供本地数据备份与恢复功能，备份介质场外存放，数据保存期限符合 6 个月规定；
b） 应制定灾难恢复预案，并进行灾难恢复演练，提高预案的执行能力；
a） 应采用热备、冷备等多种方式进行冗余备份；
c） 在灾难发生后，应根据灾难实际影响，按照预先指定的灾难恢复预案开展灾难恢复工作；
d） 应具备对平台灾难恢复的监控能力，如平台可用性和性能状态监控、灾备切换过程监控、灾备同步状态监控、灾备告警等。

8.2.4.5 应急响应

应急响应方面应符合以下要求：
a） 应制定安全事件应急响应处置预案，明确安全事件分类分级标准、响应处置人员、处置流程、处置方式、处置时效等；
b） 应定期执行应急演练计划，记录和核查应急演练结果，并根据需要修正应急响应处置预案；
c） 应做好安全事件应急资源准备，当安全事件发生时，立即启动应急处置措施，并对处置情况进行记录；
d） 安全事件处置完成后，应及时报告事件发生情况及处置情况。

8.3 技术要求

8.3.1 物理环境

一卡通应用平台应部署在非公有云平台上，平台基础设施应位于中华人民共和国境内。

8.3.2 网络通信

网络通信方面应符合以下要求：
a） 网络架构、通信传输应按照 GB/T 22239 规定的有关要求实施防护；
b） 采用密码技术实现网络通信安全，应按照 GB/T 39786—2021 中 8.2 规定的有关要求实施防护；
c） 应保持同一用户其用户身份和访问控制策略等在不同网络安全等级保护系统、不同业务系统、不同区域中的一致性；
d） 应为一卡通应用与基础支撑系统划分不同的网络区域；
e） 不同局域网之间远程通信时应采取安全防护措施，如专线、双向认证、通道加密等。

8.3.3 区域边界

8.3.3.1 边界防护

边界防护方面应符合以下要求：

a） 应通过安全隔离技术实现一卡通应用平台与基础支撑系统的隔离；
b） 应通过安全隔离技术在网络边界实现外部主机系统与一卡通应用平台主机系统的隔离；
c） 应对进出网络的数据包进行过滤，识别可疑的数据包并进行告警或者阻断；
d） 应在一卡通应用平台互联网出口部署专用的访问控制设备，并配置默认禁止等控制策略；
e） 应能够对非授权设备私自联到内部网络的行为进行检查和限制，对非授权设备，进行自动定位和封禁 IP；
f） 应能够对内部用户非授权联到外部网络的行为检查和限制，对内部用户非授权尝试连接外部网络，进行自动定位和封禁 IP；
g） 应通过安全防护设备进行风险识别及处置，对威胁情报 IP、黑客攻击等进行自动检测及封禁；
h） 应对网络层和应用层分布式拒绝服务（DDoS）攻击进行防护，对流入的数据包进行分析检测，并对发现的异常流量进行处置；
i） 应对上传下载文件的行为进行控制，防止内部人员或者外部攻击者恶意下载或者传递数据；
j） 应构建纵深防御体系，在每个关键网络边界处部署访问控制设备，采用白名单策略进行安全控制；
k） 对于部署在云平台上的一卡通应用平台，应实现东西向、南北向流量的精细化隔离，对南北向流量通过白名单方式进行限制。

8.3.3.2 访问控制

访问控制方面应符合以下要求：
a） 网络设备、安全设备应按最小安全访问原则设置访问控制权限，并删除多余或无效的访问控制规则，优化访问控制列表；
b） 应具备网络设备、安全设备的口令复杂度检测手段，对默认口令、常见弱口令、存在一定规律的口令等进行检测；
c） 应严格限制对网络设备、安全设备管理界面的访问，对异常访问请求进行记录和告警；
d） 应采取有效措施防范无线网络接入风险，措施包括绑定无线网络终端 MAC 地址、采用动态因素二次认证等方式；
e） 应在与一卡通应用平台有数据交互的外部系统网络边界设置基于协议及应用内容的访问控制措施；
f） 应采用防火墙、入侵检测等安全设备或技术，确保数据传输网络的安全性；
g） 一卡通应用平台与不同网络安全等级保护系统之间、不同业务系统之间、不同区域的系统之间、不同运营者运营的系统之间的互操作、数据交换和信息流向应进行严格控制。

8.3.3.3 入侵防范

入侵防范方面应符合以下要求：
a） 应在关键网络节点处部署可对攻击行为进行检测、阻断或者限制的防护设备，防止或者限制从外部发起的网络攻击行为；
b） 应在关键网络节点处（如核心服务器与其他内部网络区域边界处）进行严格的访问控制，部署防护设备检测、防止或限制从内部发起的网络攻击行为；
c） 应防范对一卡通应用平台的异常流量攻击，当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。

8.3.3.4 恶意代码防范

应在一卡通应用平台所涉及的网络节点部署恶意代码检测和清除产品，分析可疑的网络攻击、恶意代码、僵尸网络、病毒和蠕虫的网络传播等。

8.3.3.5 安全审计

应采取网络审计措施，监测、记录系统运行状态、日常操作、故障维护、远程运维等，留存相关日志数据不少于 6 个月。

8.3.4 应用运行环境

8.3.4.1 设备安全

设备安全方面应符合以下要求：

a） 设备应配置并启用身份鉴别和访问控制等安全措施，身份鉴别信息具有复杂度要求并定期更换；
b） 应启用设备的安全审计功能，对重要用户行为和重要安全事件进行审计，并对审计进程和审计记录进行保护；
c） 应遵循最小安装原则，关闭不需要的系统服务、默认共享和高危端口；
d） 应采用密码技术或者校验技术，对设备的资源访问控制信息、日志记录等进行完整性保护；
e） 应对未授权设备进行动态发现及管控，只允许授权的软硬件运行。

8.3.4.2 基础软件安全

8.3.4.2.1 操作系统安全

操作系统安全方面应符合以下要求：

a） 操作系统应遵循最小安装原则，仅安装一卡通应用平台所必需的服务、组件、软件等，并最小化开启业务所需的服务及端口；
b） 应采用用户名/口令等鉴别机制对操作系统用户身份进行鉴别；
c） 应设置操作系统登录延时、最大失败登录次数、锁定账号等措施，防范口令暴力破解攻击；
d） 应及时将操作系统的无用账号及默认账号清除或者锁定，不应多人共同使用一个系统账号；
e） 应设置必要的访问控制策略，授予用户完成任务所需的最小权限，限制超级管理员的访问权限，仅授予普通用户打开文件、更改指定文件的权限；
f） 应对操作系统进行安全审计，并支持操作系统日志集中收集和存储；
g） 宜选择安全的操作系统或者根据需求对操作系统及镜像进行定制，或者由第三方机构对操作系统及镜像进行安全加固；
h） 重要服务器操作系统应采用两种或者两种以上组合的鉴别技术实现用户身份鉴别，其中一种技术为密码技术。

8.3.4.2.2 数据库安全

数据库安全方面应符合以下要求：

a） 数据库系统应遵循最小安装原则，仅安装一卡通应用平台必需的服务、组件等，并最小化开启业务所需的服务及端口；
b） 应采用用户名/口令等鉴别机制实现数据库系统用户身份鉴别；
c） 应设置数据库登录延时、最大失败登录次数、锁定账号等措施，防范口令暴力破解攻击；
d） 应及时修改数据库系统的默认密码，及时将数据库系统的无用账号及默认账号清除或者锁定，一卡通应用平台访问数据库服务不应与其他应用共用同一个数据库系统账号；
e） 应设置 IP 地址白名单，仅允许指定源 IP 访问用户的数据库实例服务；
f） 应对数据库系统进行安全审计，支持日志集中收集和存储；
g） 宜选择安全数据库系统或者根据需求对数据库系统进行定制，或者由第三方机构对数据库系统进行安全加固；
h） 重要数据库系统应采用两种或者两种以上组合的鉴别技术实现用户身份鉴别，其中一种技术为密码技术。

8.3.4.2.3 中间件安全

中间件安全方面应符合以下要求：

a） 应启用身份鉴别、访问控制和安全审计等功能，不应以操作系统管理员身份启用中间件；
b） 应遵循最小安装原则，仅安装一卡通应用平台所必需的服务、组件等；
c） 应提供基于安全网络协议的接入方式，并对中间件管理控制台实施安全控制策略；
d） 应对中间件不同服务的通信提供接口安全控制，实现对会话信息的加密存储。

8.3.4.2.4 第三方组件安全

第三方组件安全方面应符合以下要求：

a） 应对第三方软件和组件的来源进行识别，选用来源可靠、版本完整稳定的第三方软件和组件，并进行策略配置和安全加固；
b） 集成应用第三方软件和组件之前，应进行分析和安全检测，确保使用的第三方软件和组件不存在已知漏洞，同时在使用过程中做好漏洞监测。

8.3.5 一卡通应用安全

8.3.5.1 身份鉴别

身份鉴别方面应符合以下要求：

a） 应符合对应用的用户进行身份标识和鉴别的要求，身份标识应具有唯一性，保证系统平台用户身份的真实性；
b） 用户口令设置应符合 6.2.2.5 a）的要求；
c） 应对登录过程中的失败、异常、风险敞口等问题采取相关措施进行处理；
d） 身份鉴别技术如采用的生物特征识别技术，应确定合理的生物特征数据采集、传输、处理、存储的方式，采取适当的措施避免生物特征数据或相关信息被非法泄露或者非法使用，采集的生物特征数据不应用于除平台身份鉴别外的其他用途。

8.3.5.2 访问控制

访问控制方面应符合以下要求：

a） 应提供专用的或者采用统一的权限管理模块实现访问控制功能，并能依据访问控制策略控制用户对客体的访问；
b） 应支持根据访问时间、访问客户端地址等条件对用户进行访问控制；
c） 应仅允许授权用户能够配置和修改访问控制策略；
d） 在有互斥业务要求的情况下，应保证有互斥业务的权限不能授予同一个业务用户。

8.3.5.3 安全审计

安全审计方面应符合以下要求：

a） 应启用安全审计功能，审计覆盖到应用的管理人员和普通用户，对其重要行为和重要安全事件进行审计；
b） 应合理分配应用日志的管理权限，不应修改日志，采用密码技术确保日志的完整性，应用日志应包括日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息等；
c） 应对应用的管理、重要业务的操作、平台配置行为进行审计，审计内容应包括管理员操作账号及权限、业务操作过程等。

8.3.5.4 入侵防范

入侵防范方面应符合以下要求：

a） 应通过设定终端接入方式或网络地址范围对通过网络进行管理的平台管理终端进行限制，并通过密码技术对登录管理终端的用户进行身份鉴别；
b） 应提供数据有效性检验功能，保证通过人机接口（如键盘、鼠标、触屏等）输入的内容符合平台设定要求；
c） 应具备对网站页面篡改、网站页面源代码暴露、穷举登录尝试、重放攻击、SQL 注入、跨站脚本攻击、钓鱼、木马以及任意文件上传、下载等已知漏洞的防范能力；
d） 应采取技术手段，对攻击活动进行检测和报警，并能将报警信息通过短信、邮件、工单等方式提醒管理人员。

8.3.5.5 客户端安全

8.3.5.5.1 APP 安全

移动应用APP安全应符合以下要求：
a） 应防止后台进程对屏幕录像盗取敏感数据，使用安全键盘输入敏感数据时按键颜色不改变，即使后台进程录屏也不能盗取 PIN、登录密码；
b） 应防止恶意程序勾取系统键盘接口盗取敏感数据，使用自绘键盘绕过系统自带键盘；
c） 应防止恶意程序读取移动操作系统文件记录每次按键坐标后重现敏感数据；
d） 应采用密码技术保护存储数据安全，确保存储数据机密性；
e） 应确保每次加密密文不重复，防止密文重放；
f） 应使用敏感数据加密方式优化短信认证流程，防止短信劫持攻击；
g） 应在第三方 SDK 嵌入前进行安全检测，严格控制第三方 SDK 权限，防止其访问除业务需要之外的数据。

8.3.5.5.2 小程序和 HTML5 安全

小程序和HTML5安全应符合以下要求：
a） 应使用键盘钩子防护，拦截键盘钩子、定时发送干扰键；
b） 应防止屏幕被截取，防止屏幕录像，拦截录屏功能；
c） 应对前台键盘驱动层和后台统一编码、加密，防止敏感数据明文传输；
d） 应对敏感数据进行加密，并对前台控件和后台统一编码、加密。

8.3.6 基础支撑系统安全

8.3.6.1 通则

一卡通应用基础支撑系统为一卡通应用服务提供基础支撑能力。社会保障卡管理信息系统、社会保障卡持卡人员基础信息库、全国社会保障卡服务平台为业务支撑系统，电子认证系统、社会保障卡密钥管理系统为安全支撑系统，均应符合8.3.6.2的要求。此外，电子认证系统还应符合8.3.6.3的要求；社会保障卡密钥管理系统还应符合10.5的要求。

8.3.6.2 通用安全防护

通用安全防护方面应符合以下要求：
b） 应加强对基础支撑系统的异常行为监测，当检测到异常时应报警，当检测到重大异常应报警并中止系统访问；
c） 应加强特权账号管理，使用分散安全管理机制，不应存在具有超级管理员权限的用户，定期审计账号使用行为，及时发现异常行为；
d） 应对基础支撑系统建立独立的安全审计功能，定义与基础支撑系统安全相关的审计事件，提供适用于基础支撑系统的安全审计设置、分析和查阅的工具。

8.3.6.3 电子认证系统安全

8.3.6.3.1 基本安全要求

电子认证系统是人力资源社会保障电子认证体系的基础设施，主要包括密钥管理系统、证书签发管理系统、证书注册管理系统和证书查验服务系统。

电子认证系统的建设和应用应符合LD/T 02—2022（所有部分）、LD/T 03—2022规定的要求。

8.3.6.3.2 数字证书数据交互安全

电子认证系统应按照附录C.2中规定的要求完成社会保障卡一卡通非对称认证应用制卡过程中的数字证书数据交互。

8.3.6.3.3 系统运行安全

电子认证系统运行安全要求主要包括物理安全、制度安全、人员安全、系统安全、通信安全、密钥安全、证书管理安全、安全审计和应用安全等，应符合LD/T 03—2022中8.3的规定。

8.3.7 接入安全

8.3.7.1 通则

一卡通应用平台在输出办事凭证、支付结算、待遇发放等应用能力时，一卡通应用系统需通过一卡通应用平台输出的接口能力进行对接，需从身份认证安全、接口交互安全、调用权限控制、通信安全、安全审计、异常监测等方面进行要求。 服务接入方应根据GB/T 22239要求，进行服务相关系统的等级保护定级、备案和测评工作。

8.3.7.2 身份认证安全

身份认证安全方面应符合以下要求：

a) 应对一卡通应用系统进行基于密码技术的有效身份鉴别，保证接入服务的真实性；
b) 不应以编码的方式将私钥明文（或者密文）编写在应用程序相关代码中；
c) 一卡通应用系统身份认证应具备防重放机制。

8.3.7.3 接口交互安全

接口交互安全方面应符合以下要求：

a) 应采用校验码技术或者密码技术保证与其他系统（或者服务）交互的鉴别信息和一卡通业务数据在传输过程中的完整性；
b) 应采用密码技术保证与其他系统（或者服务）交互的鉴别信息和一卡通业务数据在传输过程中的保密性；
c) 应对一卡通应用系统传输的个人信息、支付敏感信息等使用抗抵赖机制；
d) 一卡通应用平台需对一卡通应用系统跨安全域间的接口调用采用安全通道、防重放等安全措施；
e) 一卡通应用平台应根据安全策略限制同一时间内并发访问同一接口的系统（或者服务）数量；
f) 应对其他通过系统（或者服务）传输的数据进行有效性及合法性验证，确保输入的内容符合一卡通应用平台设定要求。

8.3.7.4 调用权限控制

调用权限控制方面应符合以下要求：

a) 应验证输入参数的合法性，在一卡通应用系统调用前应增加鉴权机制；
b) 应限制一卡通应用平台对外开放服务接口的范围，应只包含所需的最小业务功能集；

c) 应根据接口访问控制策略限制接入系统（或者服务）对客体的访问权限。

8.3.7.5 通信安全

通信安全方面应符合以下要求：

a) 应使用专线或者强壮的安全协议，例如使用安全套接字层或者传输层安全协议、互联网安全协议等；
b) 在使用 SSL/TLS 协议时，应使用安全的协议版本，不应使用弱加密套件；
c) 对于互联网协议，宜采用 IPv6，可采用 IPv4。

8.3.7.6 安全审计

安全审计方面应符合以下要求：

a) 应对一卡通应用平台的接口访问进行审计，对接入系统（或者服务）的请求和接入后的操作轨迹进行记录；
b) 应对各项审计记录进行保护，确保审计记录不可更改，审计记录保存时间不少于 6 个月。

8.3.7.7 异常监测

异常监测方面应符合以下要求：

a) 应对一卡通应用平台资源使用情况、连接数、网络带宽等运行状态进行监测；
b) 应对一卡通应用系统未授权访问、访问特征变化等异常行为进行监测和报警；
c) 应对命令执行、代码执行、SQL 注入、跨站攻击等攻击行为进行监测和报警；
d) 应具备对日志记录、监测和报警数据进行统计、分析的功能；
e) 支持对请求参数类型、参数值、字段长度、请求体大小、请求参数个数等异常检测。

9 一卡通数据安全要求

9.1 通则

一卡通数据主要包括基础数据、卡服务数据和应用数据。基础数据指人力资源和社会保障部门通过基础支撑系统为一卡通应用服务提供基础支撑能力时所处理的数据。卡服务数据指人力资源和社会保障部门、社会保障卡服务银行、第三方机构和社会保障卡制作商等主体，提供社会保障卡制作、签发、补换、注销等服务时所处理的数据。应用数据指人力资源和社会保障部门、应用机构、社会保障卡服务银行等主体提供办事凭证、支付结算和待遇发放应用时所处理的数据，包括业务数据和应用场景数据，其中业务数据遵照相关业务部门和应用机构的安全要求。一卡通数据应至少符合以下基本要求：

a) 一卡通数据安全应符合 GB/T 35273—2020、GB/T 37988—2019、GB/T 40660—2021、GB/T 41479—2022、GB/T 41803.1 的要求；
b) 定期开展数据安全审计，审计报告保存至少 2 年；
c) 关键信息基础设施的数据处理，应符合 GB/T 39204 的要求；
d) 个人信息与重要数据原则上应存储于中华人民共和国境内，确需向境外提供的，应遵循国家相关法律法规和标准的要求。

9.2 基础数据安全

9.2.1 数据收集

基础数据收集是指人力资源和社会保障部门提供一卡通产品或者服务过程中，通过线上或者线下方式，直接或者间接从数据主体，以及其他政府部门、社会保障卡服务银行、第三方机构等外部主体收集

数据的过程。数据收集过程的基础安全除应符合GB/T 41479—2022中5.2的相关要求，还应符合以下要求：

a) 应遵循合法、正当、必要的原则，不应窃取或者以其他非法方式收集数据，收集的数据应与提供的产品或服务直接相关，并与隐私政策中约定收集的内容保持一致，不应超范围采集数据；
b) 应采取技术手段对收集的数据进行质量管理和监控，确保收集的数据的准确性、一致性和完整性；
c) 应建立数据分类分级打标或数据资产管理工具，实现对个人信息、敏感个人信息、重要数据等的自动标识、标识结果发布、审核等功能；
d) 通过线下方式提供一卡通产品或者服务，收集个人信息应通过制度公开、纸质文件等方式告知，获取个人信息主体授权同意，并保留相关记录；
e) 通过 APP、小程序、公众号等线上方式提供一卡通产品或者服务，收集个人信息应符合 GB/T 35273—2020 中第 5 章、GB/T 41391 的相关要求。

9.2.2 数据传输

各级人力资源和社会保障部门进行一卡通数据传输应符合以下要求：

a) 人力资源和社会保障部门内的数据传输，原则上应通过业务专网联机完成，不具备业务专网条件的单位，可采取脱机方式，通过移动存储介质等离线方式进行交换；上下级人力资源和社会保障部门的公共服务系统间，在确保网络安全的前提下，可通过互联网接口服务方式实现公共服务数据调用；
b) 数据源端应根据待传输数据的类别、级别、规模、数据接收方以及相关要求，执行相应的数据安全保护措施；
c) 应采用密码技术等方式，确保数据传输的机密性、完整性、抗抵赖性；
d) 传输数据的两端系统应具备在数据传输前对远端系统进行身份鉴别和认证的功能，确保传输数据的双方合法可信；
e) 应对数据传输过程进行日志记录，确保数据传输过程可追溯和可审计；
f) 传输敏感个人信息和重要数据的，数据接收方系统应符合 GB/T 22239 中等级保护第三级的相关要求。

9.2.3 数据存储

9.2.3.1 逻辑存储

9.2.3.1.1 通用要求

存储一卡通数据应符合以下要求：

a) 数据存储应符合最小必要原则；
b) 应根据待存储数据的类别、级别及相关要求，执行相应的数据安全保护措施。敏感个人信息和重要数据应加密存储，使用的密码技术应遵循密码相关国家标准和行业标准；
c) 应根据业务连续性要求、数据分类分级要求，制定数据备份策略和恢复策略，同时采用数据备份与恢复的统一技术工具，保证相关工作的自动执行；
d) 系统容灾备份应符合 8.2.4.4 的相关要求；
e) 应采取技术手段保障备份和归档数据的安全，包括但不限于对备份和归档数据的访问控制、压缩或加密管理、完整性和可用性管理，确保备份和归档数据的安全和存储空间的有效利用；
f) 应定期对备份数据的有效性和可用性进行检查，定期对重要备份业务数据进行恢复验证，根据介质使用期限及时转储数据，确保数据可用性。

9.2.3.1.2 社会保障卡持卡人员基础信息库数据存储

人力资源和社会保障部门管理的社会保障卡持卡人员基础信息库数据存储应符合以下要求：

a) 应遵循最小必要原则，严格限制应用对持卡库的访问，如非必要，不提供持卡库中原始数据；
b) 应对持卡库中所存储的个人信息进行加密存储；
c) 原则上不应直接存储生物特征识别原始信息，经个人信息主体单独书面授权同意的除外，确需存储个人生物特征识别信息的，应符合 GB/T 35273—2020 中 6.3、GB/T 40660—2021 中第 6 章的相关要求；
d) 持卡库备份数据库应严格限制访问，仅在开展校验以及应用数据恢复时允许访问。

9.2.3.2 存储介质

数据存储介质应符合以下要求：

a) 通过磁盘、光盘、纸质文件等物理存储介质存储数据的，应由专人负责收发、登记、传递和保管，并通过双人双锁等方式保障存储介质的安全；
b) 除政府建设的政务云外，生产、灾备系统环境不应借用、租用其他第三方数据存储介质存储或者处理个人信息主体原始个人信息、敏感个人信息，原已借用、租用的，应至少将数据盘单独购入，或者在归还前将数据盘消磁。生产、灾备系统环境借用、租用第三方数据存储介质存储或者处理公开信息的，开发、测试系统环境借用、租用第三方数据存储介质的，归还之前应确保数据彻底清除且无法恢复。

9.2.4 数据加工和使用

9.2.4.1 数据加工

数据加工是指各级人力资源和社会保障部门基于业务优化、市场分析等需求对数据进行分析、挖掘等操作，数据加工应符合以下要求：

a) 数据加工原则上应在业务专网环境中进行，确需在其他环境使用原始数据的，需在保障安全的前提下开展；
b) 应根据待加工数据的类别、级别及要求，执行相应的数据安全保护措施，包括但不限于加密、脱敏等技术措施，保证数据加工过程的数据安全性；
c) 数据加工平台在分析任务完成后应立即删除原始数据；
d) 应对数据加工过程进行必要的监督和检查，确保加工过程的数据安全性；
e) 应对数据加工过程进行日志记录，确保数据加工过程可审计和可追溯；
f) 在开展数据加工的过程中，知道或者应当知道可能危害国家安全、公共安全、经济安全和社会稳定的，应立即停止加工活动。

9.2.4.2 自动化决策、用户画像和信息合成

利用数据进行自动化决策、用户画像和信息合成应符合以下要求：

a) 应当保证决策的透明度和结果公平合理；
b) 利用个人信息进行自动化决策的，应建立健全人工干预和用户自主选择机制，并符合 GB/T 35273—2020 中 7.7 的相关要求；
c) 应限制个人画像的使用，不应基于生物识别特征信息生成用户画像，注重用户画像的合法性，避免精确定位到特定个人，并符合 GB/T 35273—2020 中 7.4 的相关要求；
d) 利用算法自动合成文字、图片、音视频等信息，应进行明确告知并进行标识；
e) 使用生物特征识别信息进行算法精度优化等，应彻底去除与个人信息主体的身份关联，充分评估安全风险，并在使用目的完成后及时删除相关信息。

9.2.4.3 数据汇聚融合

地方一卡通数据向全国一卡通应用平台汇聚融合应符合以下要求：

a) 汇聚融合的数据不应超出采集时所声明的使用范围，因业务需要确需超范围使用个人信息的，应事先再次征得个人信息主体明示同意，并符合 GB/T 35273—2020 中 7.6 的相关要求；
b) 涉及第三方机构合作的，应以合同协议等方式明确用于汇聚融合的数据内容和范围、结果用途和知悉范围、各合作方数据保护责任和义务，以及数据保护要求等；
c) 汇聚融合前应根据汇聚融合后可能产生的数据内容、所用于的目的、范围等开展数据安全影响评估，并采取适当的技术保护措施。根据待汇聚融合数据的类别、级别以及相关要求，采用技术手段如多方安全计算、联邦学习、数据加密等技术降低数据泄露、窃取等风险；
d) 应对数据汇聚融合过程进行日志记录，确保数据汇聚融合过程可追溯和可审计；
e) 不应使用生物特征识别对比信息作为汇聚融合的直接关联点；
f) 在开展数据汇聚融合的过程中，知道或者应当知道可能危害国家安全、公共安全、经济安全和社会稳定的，应立即停止汇聚融合活动。

9.2.4.4 人脸识别数据使用

人脸识别数据的使用应符合GB/T 41819—2022中第8章和GB/T 41803.1的相关要求。

9.2.5 数据提供

对外提供数据包括委托处理和共享转让，应符合以下要求：
a) 制定数据提供管理制度，明确数据提供策略以及接收方数据安全保护要求；
b) 在对外提供数据前，应开展数据安全影响评估，确认数据内容不超出其授权范围，数据安全保护强度不因数据对外提供而降低；
c) 准确记录和保存数据提供情况，包括日期、规模、用途，以及数据应用方基本情况等；
d) 应定期对数据接收方的数据安全保护能力进行评估，当数据接收方丧失数据安全保护能力应具备启动应急响应处理能力；
e) 委托第三方开展数据处理活动的，应通过合同等形式明确约定委托处理的目的、期限、处理方式、数据种类、保护措施、双方权利和义务，以及第三方返还或者删除数据的方式等，要求第三方以合同中约定的形式返还、删除接收和产生的数据，并对数据处理活动进行监督；
f) 共享转让数据的，应与数据接收方通过合同协议等方式，明确双方在数据安全方面的责任及义务，并约定共享数据的内容和用途、使用范围等；
g) 发生收购、兼并、重组、破产时，数据接收方应继续履行相关数据安全保护义务，没有数据接收方的，应删除数据；
h) 对外提供个人信息应符合 GB/T 35273—2020 中 9.1、9.2 和 9.3 的相关要求；
i) 应确保敏感个人信息及重要数据经过脱敏后共享转让，生物特征信息原则上不应共享转让；
j) 委托第三方处理生物特征信息时，应预先向个人信息主体告知第三方相关信息、所涉生物特征信息的类型和数量、委托处理的目的；
k) 向其他政府部门共享数据的，应依据人力资源和社会保障部政务信息资源共享目录，通过部省两级外部数据交换平台，实现统一出入口共享。因业务急需且外部数据交换平台暂时无法实现的，应由同级信息化综合管理机构在保证安全的前提下，通过业务专线等其他方式实现。

9.2.6 政务数据公开

人力资源和社会保障部门进行政务数据公开应符合以下要求：
a) 应采取合理的安全管控机制和技术措施，包括但不限于网页防篡改、数据脱敏等，确保数据公开过程中的保密性、完整性和可用性；
b) 应对数据公开披露情况进行记录和保存，包括公开披露的日期、规模、目的、内容和公开范围等；

c) 个人信息原则上不应公开披露，取得个人信息主体单独同意的除外，并应符合GB/T 35273—2020中9.4的相关要求；
d) 不应公开披露生物特征数据；
e) 不应公开会对国家安全、公共利益产生重大影响的数据。

9.2.7 数据销毁

人力资源和社会保障部门数据销毁除应符合GB/T 37988—2019中11.1.2.3和11.2.2.3的相关要求，还应符合以下要求：

a) 应根据一卡通数据使用情况，制定完整数据销毁制度，确保长期存储数据、临时存储数据及备份数据的销毁要求；
b) 对达到存储期限、产品和服务停止运营、数据主体要求删除、合同约定及法律规定应该删除数据等情形，应采取技术手段，在产品和服务所涉及的系统中实现对数据进行有效销毁，防止因对存储介质中的数据进行恢复而导致的数据泄露风险，确从技术上难以实现的，应当停止除存储和采取必要的安全保护措施之外的处理；
c) 对于磁盘文件的销毁（如云主机释放回收），应采用覆写等机制确保删除的文件不可恢复，对于磁盘等存储介质的销毁（如故障主机报废处理），应采用消磁、物理捣碎等方法确保磁盘数据的彻底销毁；
d) 应对文件及介质等销毁过程进行日志记录，确保数据销毁过程可追溯和可审计。

9.3 卡服务数据安全

9.3.1 数据收集

9.3.1.1 人力资源和社会保障部门数据收集

为提供卡服务，从数据主体处收集个人信息时，除应符合GB/T 35273—2020中5.4、GB/T 40660—2021中第5章、GB/T 41819—2022中第6章的相关要求，各级人力资源和社会保障部门还应符合以下要求：

a) 为提供卡服务，收集个人信息前应通过纸质或者电子方式，向个人信息主体告知数据收集的目的、方式、范围及个人信息处理者名称、联系方式、个人信息保存期限、个人行使法定权利的方式和程序等，获取个人信息主体授权同意；
b) 敏感个人信息主体应在完全知情的基础上自主给出清晰明确的意愿表示；
c) 应避免收集不属于该个人信息主体的生物特征信息，包括生物特征原始信息，应避免采用间接方式从非个人信息主体处获取其信息，除法律法规规定场景、保护公共利益和个人重大利益场景外，不应限定收集生物特征信息作为唯一实现业务目标的方式；
d) 为提供卡服务，通过APP、小程序、公众号等线上渠道收集个人信息时，需要进行数据缓存的，应具备数据加密存储及缓存清理功能；
e) 为提供卡服务，通过线下业务窗口的采集系统收集个人信息时，采集系统应符合等保二级及以上要求，并采用摘要、消息认证码、数字签名等技术保障采集数据的完整性；
f) 为提供卡服务，通过纸质表单收集个人信息并转换为电子数据时：
   1） 应对纸质表单的保存、查阅、复制、流转等操作进行严格的审批和记录；
   2） 在纸质表单的电子化过程中，应采取技术措施控制数据的完整性、保密性。

9.3.1.2 社会保障卡服务银行、第三方机构数据收集

为提供卡服务，受各级人力资源和社会保障部门委托的社会保障卡服务银行、第三方机构数据收集应符合以下要求：

a) 应通过合同协议等方式，明确双方在数据安全方面的责任及义务，明确数据采集范围、频度、类型、用途等，确保数据的合法合规性和真实性，必要时提供相关个人信息主体的授权；
b) 持续收集数据的，还应采取技术手段对从外部机构处收集的数据和数据源进行身份鉴别和记录，并符合 GB/T 37988—2019 的相关要求；
c) 为批量制作实体社会保障卡，第三方机构收集个人信息时：
   1） 应通过协议明确采集源和采集范围，以及双方工作职责和保密义务；
   2） 应在封闭的独立网络环境进行采集，并通过人员权限管控等方式防止数据泄露；
   3） 用于存储个人信息的存储介质应由各级人力资源和社会保障部门提供和管理；
   4） 在业务办理完成后，应立即删除采集设备保存在本地的相关个人信息，不应超出委托范围，不应违规存储、加工、使用、传播所采集的信息。

9.3.1.3 实体社会保障卡制作商数据收集

为提供卡服务，实体社会保障卡制作商数据收集应符合以下要求：
a) 应采用管理或技术手段，对获取的信息源进行鉴别；
b) 应仅采集为制作实体社会保障卡而收集的数据，同时建立校验机制，保障所获得的数据的真实性、准确性；
c) 应对采集过程进行日志记录，保障数据来源的可追溯性。

9.3.2 数据传输

9.3.2.1 人力资源和社会保障部门数据传输

为提供卡服务，各级人力资源和社会保障部门数据传输应符合以下要求：
a) 各级人力资源和社会保障部门与其他政府部门、社会保障卡服务银行之间的数据传输，应符合相关行业主管单位的要求；
b) 社会保障卡管理信息系统向银行开户系统等相关系统传输符合《中华人民共和国反洗钱法》等法律法规要求的相关个人信息的，应与社会保障卡服务银行协商，并采用身份鉴别、摘要、消息认证码、数字签名、加密等技术保障传输数据的完整性和保密性；
c) 通过磁盘、光盘等硬拷贝方式传输数据，应由专人负责收发、登记、传递和保管，传递过程可采取密封等方式确保传输介质的安全；
d) RA 系统应依据 CA 系统的接口规范与数据传输规则（见附录 C.3）进行接口调用及数据传递，以确保制证数据的安全；
e) 对于因系统故障或者其他特殊情况而导致数据传递失败的，RA 系统应做好相关日志的记录，在通信恢复正常后，重新按照约定进行数据传递；
f) 制证申请数据传递时应进行加密保护，地方人力资源和社会保障部门使用电子认证应用密码机对申请数据进行加密后，再将加密后的数据通过 RA 系统传递给 CA 系统，以防用户身份信息泄露和传输中数据被篡改或丢失；
g) 制证结果数据传递时应进行加密保护，防止传输中数据被篡改或丢失。CA 系统进行加密后，将证书结果数据传递给地方人力资源和社会保障部门，地方人力资源和社会保障部门先调用电子认证应用密码机进行解密，再进行后续的数据处理。

9.3.2.2 社会保障卡服务银行、第三方机构、社会保障卡制作商数据传输

为提供卡服务，社会保障卡服务银行、第三方机构、社会保障卡制作商数据传输应符合以下要求：
a) 与其他相关方进行数据传输时，应符合人力资源和社会保障部门的安全要求；
b) 为制作实体社会保障卡，应通过专用网络等安全通道将数据传输至制卡设备。

9.3.3 数据存储

为提供卡服务，社会保障卡制作商数据存储应符合以下要求：

a) 在完成实体社会保障卡制作后，原则上不应存储卡内数据；
b) 不应对制卡数据进行查阅、修改等操作，在完成实体社会保障卡制作后 24h 内应删除保存在服务端和设备本地的制卡数据。

9.3.4 数据提供

9.3.4.1 人力资源和社会保障部门数据提供

为提供卡服务，各级人力资源和社会保障部门向他人提供数据还应符合以下要求：

a) 对提供卡服务过程中的其他合作方，应明确各方的权责，明确所提供的数据内容、方式等；
b) 社会保障卡管理信息系统涉及与银行系统进行金融数据交互的，应符合金融行业相关国家标准和行业标准；
c) 应对数据提供过程进行日志记录，确保数据共享过程可追溯和可审计。

9.3.4.2 社会保障卡服务银行、第三方机构、社会保障卡制作商数据提供

为提供卡服务，社会保障卡服务银行、第三方机构、社会保障卡制作商向他人提供从人力资源和社会保障部门获取的数据还应符合如下要求：

a) 应严格按照与人力资源和社会保障部门的约定向他人提供数据；
b) 应对数据提供过程进行日志记录，确保数据提供过程可追溯和可审计。

9.4 应用数据安全

9.4.1 数据收集

9.4.1.1 人力资源和社会保障部门数据收集

人力资源和社会保障部门输出办事凭证、支付结算、待遇发放等应用能力时，数据收集应符合以下要求：

a) 应明确应用服务中所必须收集的个人信息，并获得个人信息主体的授权同意；
b) 应制定应用机构数据约束机制，并明确数据源、数据采集范围和频度，事前开展数据安全影响评估。

9.4.1.2 应用机构数据收集

提供一卡通应用服务时，应用机构应按照与人力资源和社会保障部门的约定范围收集个人信息，并留存个人信息授权同意记录。

9.4.2 数据传输

一卡通应用平台与一卡通应用系统进行数据传输时应符合以下要求：

a) 为提供一卡通应用服务，客户端与服务端的传输应采用密码技术保护传输通道安全；
b) 传输社会保障卡卡号、社会保障号码、社会保障卡银行账户、支付信息等敏感个人信息时，应采用身份鉴别、摘要、消息认证码、数字签名、加密等技术保障个人信息的完整性和保密性；
c) 通过接口交换共享数据时应对报文全文签名；通过数据库交换共享数据时，一卡通应用平台提供只读库，数据接收方通过中间库接收数据；通过数据文件交换共享数据时，一卡通应用平台应对数据进行签名，签名与数据文件通过不同渠道发送给数据接收方；
d) 为进行灾备或者提供一卡通应用服务，通过运营商网络传输数据，应采用专线或者 VPN 等技术保障传输通道的安全。

9.4.3 数据存储

9.4.3.1 一卡通应用平台数据存储

各级人力资源和社会保障部门数据存储应符合以下要求：

a) 脱敏后的数据应与用于还原数据的恢复文件隔离存储，使用恢复原始数据的技术应经过严格审批，并留存相关审批及操作记录；
b) 原则上不应存储从持卡库调用的姓名、社会保障卡卡号、社会保障号码、社会保障卡银行账户等基础信息；
c) 应用机构确有需要在一定时间内大规模访问持卡库数据的，应向人力资源和社会保障部门提出申请，由人力资源和社会保障部门进行审批并进行人工核查。

9.4.3.2 应用机构数据存储

应用机构数据存储应符合以下要求：

a) 读卡、扫码等终端原则上不应存储从服务端获取的数据，确因业务需要存储，应设置一定的存储期限并加密存储；
b) 未经授权不应在服务端留存从一卡通应用平台获取的敏感个人信息，在业务服务完成后应立即删除。

9.4.4 数据加工和使用

各级人力资源和社会保障部门对一卡通应用平台数据进行加工和使用、应用服务业务数据在一卡通应用平台汇聚融合应符合 9.2.4 的相关要求。

9.4.5 数据提供

9.4.5.1 人力资源和社会保障部门数据提供

各级人力资源和社会保障部门向他人提供数据应符合以下要求：

a) 应通过与应用机构签订数据提供协议，约定获得数据目的和用途以及数据类型、数量、频率、方式、大小等；
b) 应约定数据提供方式，如采用接口方式提供数据，接口安全应符合 8.3.7.3 的相关要求；
c) 应对数据提供过程进行日志记录，确保数据共享过程可追溯和可审计；
d) 如提供的数据为个人信息，应开展个人信息保护影响评估，并及时告知个人信息主体，获取个人信息主体的单独同意；
e) 提供支付结算和待遇发放能力时，一卡通应用平台涉及与银行进行金融数据交互的，应符合金融行业相关国家标准和行业标准；
f) 向其他政府部门提供数据的，应制定部门数据共享清单以及共享形式，充分考虑用户数据安全情况。

9.4.5.2 应用机构数据提供

应用机构对外提供从一卡通应用平台获取的数据时应符合以下要求：

a) 应严格按照与人力资源和社会保障部门的约定对外提供数据；
b) 应对数据处理过程进行日志记录，确保数据处理共享过程可追溯和可审计。

9.4.6 数据公开

应用机构公开从一卡通应用平台获取的数据时应符合以下要求：

a) 原则上不应公开披露个人信息，取得个人信息主体单独同意的除外，并应符合 GB/T 35273—2020 中 9.4 的相关要求；
b) 公开展示个人信息时应进行脱敏处理。

9.4.7 数据销毁

应用机构销毁从一卡通应用平台获取的数据时应符合以下要求：

a) 对存在于数据库、文件系统、临时文件（cookies 等）、内存等的敏感个人信息，包括但不限于完整的电子社会保障卡卡号、社会保障号码、社会保障卡银行账户，应用机构应制定独立的数据删除机制，不依赖于操作系统或者虚拟机提供的垃圾回收机制；

b) 应用机构在退出应用合作时，应按协议约定销毁合作过程中收集或者产生的相关数据，不应保留。

10 一卡通密钥安全要求

10.1 通则

国家级一卡通密钥体系是将国家根密钥根据省、市的申请分散国家密钥为国家二级、国家三级密钥，并通过母卡分发到省、市人力资源和社会保障部门，根据省、市的申请生成PSAM卡并下装所需级别、类型的国家密钥。

省级一卡通密钥体系是生成维护省内省级密钥，导入省级母卡内的国家二级密钥，根据下属市的申请分散密钥为国家三级（省二级）密钥并通过母卡分发到市人力资源和社会保障部门，根据市的申请为PSAM卡下装所需类型的省一级或者省二级密钥。

市级一卡通密钥体系是生成维护市内市级密钥，导入市级母卡内的国家三级密钥和省二级密钥，根据需要为安全模块下装所需类型的市级密钥。

非对称密码算法、对称密码算法、杂凑算法应分别符合GB/T 32918.4 、GB/T 32907、GB/T 32905的相关要求。

10.2 密钥管理要求

密钥管理方面应符合以下要求：

a) 密钥管理主要保证密钥全生命周期的安全性，保证密钥 （除公钥外）不被非授权的访问、使用、泄露、篡改和替换，保证公钥不被非授权的篡改和替换；

b) 一卡通应用密钥体系由一卡通应用平台根据密码应用需求在密码应用方案中明确，并在密码应用实施中落实；

c) 密钥管理主要包括密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等环节；

d) 对于密钥的应用，应制定完善的密钥管理制度，包括但不限于密钥应用事件处置报告管理制度、密钥应用安全管理制度、密钥应用岗位责任制度、密钥应用上岗人员培训制度、密钥安全管理规则、人员保密制度与调离制度、人员操作规范、制度发布流程规范、密钥应用安全管理制度论证和审定记录、密钥应用操作规范论证和审定记录、密钥操作执行记录、密钥应用安全岗位人员考核记录等；

e) 对于密钥载体，应由专人进行保管，密钥载体管理人员应不少于两人，密钥载体管理人员应与密钥载体管理机构签署保密协议；密钥载体应通过专人专车的方式进行运输，确保运输过程中安全；密钥载体不应移交给第三方保管或者使用，如应由第三方进行管理的，应签署保密协议，加强监管，并明确收回期限。

10.3 社会保障 PSAM 卡管理

社会保障PSAM卡管理应符合以下要求：

a) 对于社会保障 PSAM 卡的发放，应对申请机构的业务范围、运行环境、管理制度等方面进行审核，确保符合社会保障 PSAM 卡使用条件后再进行发放；

b) 社会保障 PSAM 卡发放时，应对社会保障 PSAM 卡序列号、终端机编号、用途、使用单位（业务办理点）、相关责任人等信息进行登记并备案；
c) 社会保障 PSAM 卡使用单位应建立严格的社会保障 PSAM 卡安全管理制度，规范 PSAM 卡使用单位在领卡、用卡、销卡等环节的安全；
d) 应对社会保障 PSAM 卡的使用进行认证并监管，及时掌握社会保障 PSAM 卡的使用情况，确保社会保障 PSAM 卡的合规使用；
e) 社会保障 PSAM 卡回收、损坏、丢失或被盗后，应及时进行注销登记、销毁及黑名单处理。

10.4 硬件密钥设备安全

硬件密钥设备应符合以下要求：
a) 硬件密钥设备如密码机应使用符合 GB/T 37092 要求的密码模块；
b) 硬件密钥设备应放置在有严格管理的机房或者机柜内进行保管，并应对保管机房进行全程监控；
c) 硬件密钥设备应定期进行安全检查，包括但不限于外壳完整性、是否被拆卸、破坏以及额外连接线路或外接电缆等；
d) 硬件密钥设备销毁密钥或者密钥错误，同时数据库信息遭到破坏时，应使用母卡将完整准确的密钥重新导入到硬件密钥设备中；
e) 硬件密钥设备因自然淘汰或不可抗力造成损坏而必须更换时，应彻底销毁硬件密钥设备中的密钥。
f) 密钥卡应存放在安全区域（如机要室、档案室）的保险容器（如保险柜）内，并进行严格的出入库登记，登记记录一并存放在保险容器内。保险容器的钥匙和密码应由两名密钥载体管理人员分别管理；
g) 密钥母卡和传输密钥卡应有完全相同的两套，且应异地存放，互为备份；
h) 对密钥母卡、传输密钥卡的操作，应由两名密钥载体管理人员同时在场；
i) 密钥卡自然损坏或因不可抗力造成损坏的，应统一销毁和更换。

10.5 社会保障卡密钥管理系统安全

社会保障卡密钥管理系统应符合以下要求：
a) 社会保障卡密钥管理系统应安装在独立的计算机上，安装社会保障卡密钥管理系统的计算机应安全存放，设置开机密码，不应使用 USB 接口外设（如 U 盘、充电器等）；
b) 在生成本地密钥时输入的密钥种子不应以任何形式出现在任何介质上；
c) 社会保障卡密钥管理系统的数据文件应定期备份，备份文件应一式两份并进行异地保管；
d) 安装社会保障卡密钥管理系统的计算机因自然淘汰或者不可抗力造成损坏而必须更换时，应彻底清除硬盘上的相关数据文件并销毁硬盘。

10.6 卡载体密钥安全

卡载体密钥应符合以下要求：
a) 卡内密钥应具备独立性，用于某种特定功能的密钥，包括保存在卡内的密钥和用于产生、派生、传输这些密钥的密钥，不能被任何其他功能所使用；
b) 卡内密钥的生成和派生应有物理随机数发生器所产生的随机数参与计算，可能产生或者使用的临时密钥，只能存放在易失性电存储介质中，电源消失后即被销毁；
c) 卡内密钥的装载和更新应采用安全报文传送，传输过程中的密钥应经过加密，不允许明文密钥以任何形式出现在传送过程中；
d) 卡内密钥不应被外界以任何形式读取，应在卡操作系统控制下用于芯片内部安全计算；
e) 应用永久锁定后，卡内与该应用相关的密钥全部失效，失效或者过期密钥不应继续使用。

10.7 终端密钥安全

终端密钥应符合以下要求：

a) 应确保一卡通终端密钥的唯一性，符合一机一密的安全要求；
b) 一卡通终端应具备对其所存储密钥的生命周期管理功能，以阻止已失效或者过期密钥的使用；
c) 一卡通终端应保证密钥在没有授权的情况下，不被泄露；同时也应保证密钥除在终端操作系统的控制下用于芯片内部的安全计算外，不应被外界直接访问；
d) 应在一卡通终端的安全存取模块内产生公私钥；
e) 一卡通终端产生的公钥应提交证书发放程序或者系统，以生成并分配证书；
f) 私钥应保存于一卡通终端的安全存取模块中，不应被导出。

附 录 A
（规范性）
实体社会保障卡安全报文的计算方法

A.1 8 字节分组密码算法 MAC 计算

按照如下方式产生MAC：

第一步：取8字节的十六进制数字‘00’作为初始变量。

第二步：按照顺序将以下数据连接在一起形成数据块：

——CLA、INS、P1、P2、Lc；

——在命令的数据域中（如果存在）包含明文或加密的数据 （例如更改 PIN，加密后的 PIN 数据块放在命令数据域中传输）；

——医疗费用结算交易 MAC 的计算不含有 CLA、INS、P1、P2、Lc 数据块。

第三步：将该数据块分成8字节为单位的数据块。最后一个数据块长度有可能不足8字节。

第四步：在数据最右边加上十六进制数字‘80’，如果达到8字节长度，则转到第五步；否则在其右边加上十六进制数字‘00’，直到长度达到8字节。

第五步：对这些数据块使用MAC过程密钥进行加密，过程密钥按照A.3描述的方式产生。

第六步：最终从计算结果左侧取得4字节长度的MAC。

A.2 16 字节分组密码算法 MAC 计算

按照如下方式产生MAC：

第一步：取16个字节的十六进制数字‘00’作为初始变量。

第二步：按照顺序将以下数据连接在一起形成数据块：

——CLA、INS、P1、P2、Lc；

——在命令的数据域中（如果存在）包含明文或加密的数据 （例如更改 PIN，加密后的 PIN 数据块放在命令数据域中传输）；

——医疗费用结算交易 MAC 的计算不含有 CLA、INS、P1、P2、Lc 数据块。

第三步：将该数据块分成16字节为单位的数据块。最后一个数据块长度有可能不足16字节。

第四步：在数据最右边加上十六进制数字‘80’，如果达到16字节长度，则转到第五步；否则在其右边加上十六进制数字‘00’，直到长度达到16字节。

第五步：对这些数据块使用MAC过程密钥进行加密，过程密钥按照A.3描述的方式产生。

第六步：将16字节运算结果按4字节分块做异或运算。取最终计算结果（4字节）作为MAC。

A.3 过程密钥计算方法

A.3.1 8 字节分组密码算法过程密钥计算

密钥对过程密钥输入数据进行加密生成过程密钥。

过程密钥输入数据是随机数，议取 8 字节，取 4 字节随机数时则补十六进制数字‘00’后达到 8 字节。

A.3.2 16字节分组长度数据密码算法过程密钥计算

密钥对过程密钥输入数据进行加密生成过程密钥。

过程密钥输入数据是随机数，建议取 16 字节随机数，取 4 字节随机数时则补 12 字节“000000000000000000000000”达到 16 字节，取 8 字节随机数时则补 8 字节“0000000000000000”达到 16 字节。

A.4 鉴别数据的计算

A.4.1 8字节分组密码算法鉴别数据计算

使用操作权限鉴别过程密钥对原始数据进行加密。

A.4.2 16字节分组密码算法鉴别数据计算

原始数据是16字节数据或者由8字节设定值补8字节十六进制数字‘00’构成，通过鉴别过程密钥对原始数据进行加密，加密结果左右“异或”运算得到鉴别数据（8字节）。

A.5 数据加密计算方法

A.5.1 8字节分组密码算法加密计算

8字节分组密码算法的加密技术如下所述：

第一步：在明文数据前加上L_D产生新的数据块；

第二步：将第一步中生成的数据块分成8字节为单位的数据块。最后一个数据块长度有可能不足8字节；

第三步：如果最后（或唯一）数据块的长度等于8字节，转到第四步；如果最后（或唯一）数据块的长度不足8字节，则在其右边加上十六进制数字‘80’，如果达到8字节长度，则转到第四步；否则在其右边加上十六进制数字‘00’，直到长度达到8字节；

第四步：每一个数据块使用数据加密过程密钥进行加密；

第五步：计算结束后，所有加密后的数据块）按照原顺序连接在一起，并将结果数据块插入到命令数据域中。

A.5.2 16字节分组密码算法加密计算

16字节分组密码算法的加密技术如下所述：

第一步：在明文数据前加上L_D产生新的数据块；

第二步：将第一步中生成的数据块分成16字节为单位的数据块。最后一个数据块长度有可能不足16字节；

第三步：如果最后（或唯一）数据块的长度等于16字节，转到第四步；如果最后（或唯一）数据块的长度不足16字节，则在其右边加上十六进制数字‘80’，如果达到16字节长度，则转到第四步；否则在其右边加上十六进制数字‘00’，直到长度达到16字节；

第四步：每一个数据块使用数据加密过程密钥进行加密；

第五步：计算结束后，所有加密后的数据块按照原顺序连接在一起，并将结果数据块插入到命令数据域中；

A.6 数据解密计算方法

A.6.1 8字节分组密码算法解密计算

8字节分组密码算法的解密技术如下：

第一步：将命令数据域中的数据块分成8字节为单位的数据块。每个数据块使用数据加密过程密钥进行解密；

第二步：将所有解密后的数据块按照顺序连接在一起。数据块由L_D、明文数据、填充字符组成；

第三步：LD 表示明文数据的长度，因此，它被用于恢复明文数据。

A.6.2 16字节分组密码算法解密计算

16 字节分组密码算法的解密技术如下：

第一步：将命令数据域中的数据块分成 16 字节为单位的数据块。每个数据块使用的数据加密过程密钥进行解密；

第二步：将所有解密后的数据块按照顺序连接在一起。数据块由 L_D、明文数据、填充字符组成。

A.7 社会保障卡密钥

社会保障卡相关密钥见表 A.1 和表 A.2。

表 A.1 SSSE 应用密钥列表

分类	密钥	用途	适用的应用范围	管理方式
-	IRK	鉴别发卡方的密钥	应用提供者	部
-	PUK	PIN 解锁密钥	发卡方	省
应用维护密钥	STK SSSE	发卡方或应用提供者用于产生应用锁定、卡片锁定和读取或更新二进制或记录命令的 MAC	发卡方	部
	STKDF01		公共应用	部
	STKDF02		就业与失业应用	部
	STKDF03		社会保险 1 应用	部
	STKDF04		社会保险 2 应用	部
	STKDF07		人事与人才应用	部
卡片或应用锁定控制密钥	BK	发卡方或应用提供者控制锁定卡片或应用操作的密钥	发卡方	省
	LKDF03		社会保险 1 应用	省
	LKDF04		社会保险 2 应用	省

表 A.1　SSSE 应用密钥列表（续）

分类	密钥	用途	适用的应用范围	管理方式
	UK_{SSSE}		发卡方和持卡人基本信息	省
	$UK1_{DF01}$		户籍信息	省
	$UK2_{DF01}$		个人状况信息	省
	$UK3_{DF01}$		婚姻状况信息	部
	$UK4_{DF01}$		通讯信息	部
	$UK5_{DF01}$		国家/地区及政治面貌信息	省
	$UK6_{DF01}$		学历信息	部
	$UK7_{DF01}$		预留信息 1	部
	$UK8_{DF01}$		预留信息 2	部
	$UK9_{DF01}$		预留信息 3	部
	UKA_{DF01}		预留信息 4	部
	UKB_{DF01}		预留信息 5	部
	$UK1_{DF02}$		职业和专业技能信息	部
	$UK2_{DF02}$		就业状况信息	省
	$UK3_{DF02}$		就业记录	省
应用数据	$UK4_{DF02}$	发卡方或应用提供者控制	就业创业证信息	部
更新密钥	$UK5_{DF02}$	应用数据更新操作的密钥	就业援助对象认定信息	部
	$UK6_{DF02}$		就业扶持政策享受信息	部
	$UK1_{DF03}$		失业保险信息	省
	$UK2_{DF03}$		劳动能力鉴定信息	部
	$UK3_{DF03}$		养老保险信息	部
	$UK4_{DF03}$		工伤保险信息	部
	$UK5_{DF03}$		生育保险信息	部
	$UK6_{DF03}$		工伤认定信息	部
	$UK7_{DF03}$		供养亲属信息	部
	$UK8_{DF03}$		参保凭证信息	部
	$UK1_{DF04}$		医疗、工伤、生育保险基本信息	省
	$UK2_{DF04}$		医疗保险临时脱网结算信息	部
	$UK1_{DF07}$		荣誉信息	部
	$UK2_{DF07}$		专家信息	部
	$UK3_{DF07}$		军队转业干部信息	部

表 A.1　SSSE 应用密钥列表（续）

分类	密钥	用途	适用的应用范围	管理方式
医疗保险交易密钥	DLK	用于产生账户划入交易中使用的过程密钥 SESLK，在账户划入交易中计算 MAC	医疗保险账户划入交易	省
	DPK	用于产生医疗费用结算中使用的过程密钥 SESPK，在医疗费用结算交易中计算 MAC	医疗保险医疗费用结算交易	部
	DSK	用于更新年度起始日期的密钥	更新年度起始日期	省
	DTK	用于产生账户支付、个人自付和统筹基金支付交易中使用的 TAC	医疗保险交易	省
应用数据读取密钥	RK_{SSSE}	发卡方或应用提供者控制部分应用数据读取操作的密钥	指纹和相片信息	部
	$RK1_{DF01}$		公共应用信息	部
	$RK1_{DF02}$		就业与失业信息	部
	$RK1_{DF03}$		养老、工伤、生育保险信息	部
	$RK2_{DF03}$		失业保险信息	部
	$RK1_{DF04}$		医疗保险和医疗费用结算信息	部
	$RK1_{DF07}$		荣誉信息	部
	$RK2_{DF07}$		专家信息	部
	$RK3_{DF07}$		军队转业干部信息	部

表 A.2　ACSE 密钥列表

分类	密钥	用途	适用的应用范围	管理方式
-	MK_{ACSE}	控制非对称认证系统环境 ACSE 下文件读写	应用索引	
			设备信息	
-	MK_{DF01}	控制社会保障证书应用读写	文件索引	
			容器索引	
-	PIN	控制容器公私钥、证书文件读写	公、私钥	
			证书	

附 录 B
（规范性）
电子社会保障卡服务渠道接入安全技术规范

B.1 范围

本文件规定了电子社会保障卡服务渠道接入的安全技术要求。

本文件适用于电子社会保障卡服务渠道开发、集成、应用、维护及运营过程，可作为电子社会保障卡服务渠道以及检测机构的技术要求。

B.2 电子社会保障卡服务渠道安全

B.2.1 系统安全

电子社会保障卡服务渠道应根据 GB/T 22239 的相关要求，进行整体系统（包括客户端和后台服务端）的等级保护定级、备案和测评。

B.2.2 第三方组件安全（客户端）

电子社会保障卡服务渠道客户端应避免使用存在已知漏洞的系统组件、第三方组件。

电子社会保障卡服务渠道客户端在使用第三方组件时，应禁止第三方组件未经授权收集客户端信息和个人信息。

B.2.3 SDK版本安全（客户端）

电子社会保障卡服务渠道调用的电子社会保障卡 SDK 版本应及时升级，确保为最新版本。

B.2.4 HTML5页面安全（客户端）

电子社会保障卡服务渠道客户端在使用电子社会保障卡HTML5页面方式实现部分功能时，不应篡改HTML5页面。

B.2.5 会话有效期（客户端）

电子社会保障卡服务渠道登录状态不应长期有效，超过一定期限（最长72h）应强制用户重新登录。

B.2.6 抗攻击能力（客户端）

电子社会保障卡服务渠道客户端应具备基本的抗攻击能力。

电子社会保障卡服务渠道客户端安装、启动、更新时应对自身的完整性和真实性进行校验。

B.2.7 抗攻击能力（服务端）

电子社会保障卡服务渠道服务端的存储和运行环境应为专用的机房。

电子社会保障卡服务渠道服务端应具有逻辑边界，应采用有效的技术手段对跨越边界的访问进行控制、鉴别和记录。

电子社会保障卡服务渠道服务端应探测、阻止并记录未经授权的访问。

电子社会保障卡服务渠道服务端安装、启动、更新时应对自身的完整性和真实性进行校验。

电子社会保障卡服务渠道服务端应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。

B.2.8 环境校验（客户端）

电子社会保障卡服务渠道客户端启动时应执行自检程序，检查客户端运行时所必须的条件，在用户知情的情况下能向服务端反馈设备信息等情况。

B.2.9 下载更新安全（客户端）

当需要远程下载应用时，电子社会保障卡服务渠道应采取有效手段保证客户端传输过程的机密性和客户端的完整性。

电子社会保障卡服务渠道客户端安装过程中，应拥有独立的安装目录，唯一的应用标识符，明确的版本序号，不应篡改、覆盖、删除系统文件和其他软件。

B.2.10 用户个人信息保护

电子社会保障卡服务渠道在收集、使用用户信息之前，应明示收集、使用信息的目的、方式和范围，公开其收集、使用规则，并取得用户的授权同意。

未经用户同意，也未做匿名化处理，电子社会保障卡服务渠道不应直接向第三方提供个人信息。

B.2.11 审计安全

电子社会保障卡服务渠道应记录一定时期内（如 3 个月）全部用户访问日志。

电子社会保障卡服务渠道应通过行业标准日志文件格式存储记录，并对日志进行集中管理。

B.3 数据安全

电子社会保障卡服务渠道在身份认证结束后不应存储敏感数据。

电子社会保障卡服务渠道客户端与服务端间的交易报文，应采用数字证书全报文或关键数据域签名和验签，保证报文的真实性和不可抵赖性。

电子社会保障卡服务渠道应确保敏感数据传输时不应仅依赖协议层加密，应在应用层加密后才可进行传输。

电子社会保障卡服务渠道客户端不应留存从全国社保卡服务平台获取的敏感数据。

敏感数据在使用完成后应进行有效销毁。

B.4 通信安全

电子社会保障卡服务渠道的服务端与客户端、服务端与全国社会保障卡服务平台或客户端与全国社会保障卡服务平台通信时，应使用专线或强壮的安全协议，宜采用 IPv6，可采用 IPv4。

在使用 SSL/TLS 协议时，应符合全国社会保障卡服务平台支持的最低版本，应使用安全的版本，不应使用存在安全隐患版本以及弱加密套件。

电子社会保障卡服务渠道客户端与服务端应具备合法性认证机制，通过签名验签等密码技术手段进行双向认证，确保合法性。

B.5 密码算法安全

B.5.1 密码算法

密码算法的选择和使用宜符合国家密码管理部门的要求及电子社会保障卡的设计要求。

B.5.2 加密算法安全

应使用对称加密算法、非对称加密算法对认证信息和敏感数据进行加密保护。对于使用对称加密算法的单次应用或交易，为避免攻击者通过获取明文密文组对密钥进行字典攻击，应使用密钥变换的方法生成一次性密钥，以对设备或客户端主密钥进行保护。应定时重新协商会话密钥。

宜使用以下算法和参数：

——SM4；

——SM2，使用 256 位长度的私钥。

B.5.3 密钥加密或解密

可使用对称加密算法、非对称加密算法用于不安全信道的密钥分发。

宜使用以下算法和参数：

——SM4；

——SM2，可使用 256 位长度的私钥。

B.5.4 安全散列（消息摘要）

宜使用 SM3 算法进行消息摘要。

B.5.5 数字签名

应使用适当的杂凑算法配合非对称签名算法进行数字签名计算。宜使用非对称数字签名技术对用户身份或关键数据进行认证。应正确使用密钥管理规则以确保私钥的机密性和私钥、公钥的完整性及真实性。

宜使用 256 位长度私钥的 SM 算法。

B.6 接口安全

电子社会保障卡服务渠道应通过全国社会保障卡服务平台分配的渠道账户访问电子社会保障卡文档库，获取 SDK、H5 及 API 接口文件。电子社会保障卡服务渠道应将获取的接口文件保存在内部网络，遵循“最小权限”原则，防止接口文件泄露。

电子社会保障卡服务渠道应提示用户授权电子社会保障卡服务渠道及全国社会保障卡服务平台获取运行环境物理信息、地理位置信息，并应允许全国社会保障卡服务平台获取经用户授权信息。

为确保调用安全，电子社会保障卡服务渠道服务端调用相关接口时，应按照全国社会保障卡服务平台接口文档要求传入参数。

电子社会保障卡服务渠道客户端应对接口进行保护，防止其他应用对电子社会保障卡服务渠道客户端接口进行非授权调用；电子社会保障卡服务渠道客户端应对传入的 URI 进行校验与安全处理，防止电子社会保障卡服务渠道客户端运行异常或操作异常。

电子社会保障卡服务渠道客户端正式版不应调用测试接口。

B.7 密钥管理

电子社会保障卡服务渠道使用的硬件加密设备或软件加密模块应符合国家密码管理部门的相关要求。

电子社会保障卡服务渠道客户端不应存储 AK、SK、DK 等密钥。

电子社会保障卡服务渠道应采用必要手段保护服务端密钥的全生命周期安全。

电子社会保障卡服务渠道应采用必要手段保护电子社会保障卡服务渠道的密钥及密钥加密密钥。

电子社会保障卡服务渠道应保护任何用于加密重要信息数据以防泄露和滥用的密钥及其密钥加密密钥。

B.8 业务处理环境管理

电子社会保障卡服务渠道服务端应具有独立的测试环境，用于系统版本升级前的测试，及配合全国社会保障卡服务平台的变更而进行的验证和联调测试。

B.9 电子社会保障卡服务渠道软件管理

电子社会保障卡服务渠道应保证开发过程的安全性，并将信息安全纳入整个软件开发生命周期。

电子社会保障卡服务渠道的开发应避免由软件漏洞引发的安全风险。

电子社会保障卡服务渠道不应限制数据库服务器和应用服务器部署在同一台设备上，不应降低关联服务器的安全性。

电子社会保障卡服务渠道发布之前应进行严格测试，以确定不存在安全威胁和漏洞。

电子社会保障卡服务渠道的发布版本应由配置管理人员进行生成、发布和登记。

电子社会保障卡服务渠道与应用发布机构之间在传输应用程序源代码及数据时，应建立安全通道，保证数据传输的机密性和完整性。

电子社会保障卡服务渠道应提供业务开展的服务/端口记录表。

电子社会保障卡服务渠道应提供对客户端、服务端与数据库进行安全存取的操作指南，并且在指南中应明确使用唯一的用户名与安全验证方法的要求。

电子社会保障卡服务渠道进行变更时，应遵循变更控制程序，以确保变更不会影响系统的功能及安全性。

附 录 C
（规范性）
社会保障卡一卡通非对称认证应用制卡数据流转规范

C.1 范围

本文件规定了社会保障卡一卡通非对称认证应用制卡有关环节的流程，以及用于交换的文件命名规范、数据标准等。

本文件适用于电子认证系统、制卡系统、快速发卡系统、业务系统等各系统在制卡过程中的数字证书数据交互。

C.2 技术要求

非对称认证应用制卡数据主要分为两类：一是数字证书申请数据，在证书申请阶段形成；二是数字证书及密钥等数据，在证书签发后形成。报盘/回盘文件传输方式主要包括以下方式：

a) 通过人工方式进行数据交互，人力资源和社会保障部门工作人员可登录省级 RA 系统，通过页面上传报盘文件、下载回盘文件；回盘文件下载后，采用安全方式将其返回给卡商或个人化中心；

b) 通过 FTP 方式进行文件传输，人力资源和社会保障部门工作人员通过远程桌面或 FTP 登录到省级 RA 系统指定的服务器，将报盘文件拷贝到指定目录下，并在指定的回盘目录中复制回盘文件；回盘文件获取后，采用安全方式将其返回给卡商或个人化中心；

c) 地方人社系统通过调用省级 RA 系统的服务接口，完成报盘文件和回盘文件下载。

数据交互过程中应符合以下要求：

a) 文本采用 UTF-8 进行编码，以防文件中的中文出现乱码，造成程序解析失败；

b) 报盘文件传递时须进行加密保护，地方人力资源和社会保障部门使用电子认证应用密码机对报盘文件进行加密，再将加密后的文件传递给电子认证系统，以防用户身份信息泄露和传输中数据被篡改或丢失；

c) 回盘文件传递时须进行加密保护，防止传输中数据被篡改或丢失。电子认证系统进行加密后，将文件传递给地方人力资源和社会保障部门，地方人力资源和社会保障部门先调用电子认证应用密码机进行解密，再进行后续的数据处理。

C.3 接口规范

接口的入参和出参均为密文，由快速发卡系统或业务系统调用电子认证应用密码机，完成对入参数据的加密和出参数据的解密。

a)证书注册 certRegister

证书注册接口规范见表 C.1。

表 C.1 证书注册接口规范

功能简介	证书注册，根据证书注册信息，签发证书并返回。
接口名称	String certRegister(String registerParameter, String sysCode)

表 C.1 证书注册接口规范（续）

参数说明	
入参说明	registerParameter：证书申请数据采用字符串数据类型，以密文方式进行数据传输，加密方式请参考 GM/T 0010—2012《SM2 密码算法加密签名消息语法规范》9.1 数字信封章节。 证书申请数据明文如下。 ——<XM>姓名</XM> ——<KH>卡号</KH> ——<SHBZHM>社会保障号码</SHBZHM> ——<QMGY>签名公钥</QMGY> ——<SF>算法</SF> ——<XZQHDM>发卡地区行政区划代码</XZQHDM> sysCode：当前发起请求业务系统的系统代码 ID，通过协商后，统一规划的业务系统代码，必填项
返回值	返回一个字符串，内容解释如下。 <STATE>0 或 1</STATE> <ERRORCODE>1000</ERRORCODE> <QMZS>签名证书</QMZS> <JMZS>加密证书</JMZS> <JMMY>加密密钥</JMMY> <ZKMY>主控密钥</ZKMY> <GLYPIN>管理员 PIN</GLYPIN> 标记说明： <STATE>操作状态：0=成功，1=失败 <ERRORCODE>错误代码 <QMZS>签名证书 <JMZS>加密证书 <JMMY>加密密钥密文 <ZKMY>主控密钥 <GLYPIN>管理员 PIN

b)证书查询 certQuery

证书查询接口规范见表 C.2。

表 C.2 证书查询接口规范

功能简介	证书查询，根据持卡人和卡片信息查询证书并返回。
接口名称	String certQuery(String queryParameter, StringsysCode)

表 C.2 证书查询接口规范（续）

参数说明	
入参说明	queryParameter：查询条件内容，采用字符串数据类型，以密文方式进行数据传输，加密方式请参考国家密码管理局 GM/T 0010—2012《SM2 密码算法加密签名消息语法规范》9.1 数字信封章节。 证书查询数据明文如下。 ——<XM>姓名</XM> ——<KH>卡号</KH> ——<SHBZHM>社会保障号码</SHBZHM> ——<XZQHDM>发卡地区行政区划代码</XZQHDM> sysCode：当前发起请求业务系统的系统代码 ID，通过协商后，统一规划的业务系统代码，必填项
返回值	返回一个字符串，内容解释如下。 <STATE>0 或 1</STATE> <ERRORCODE>1000</ERRORCODE> <QMZS>签名证书</QMZS> <JMZS>加密证书</JMZS> <JMMY>加密密钥</JMMY> <ZKMY>主控密钥</ZKMY> <GLYPIN>管理员 PIN</GLYPIN> 标记说明： <STATE>操作状态：0=成功，1=失败 <ERRORCODE>错误代码 <QMZS>签名证书 <JMZS>加密证书 <JMMY>加密密钥密文 <ZKMY>主控密钥 <GLYPIN>管理员 PIN

c)证书注销 certRevoke

证书注销接口规范见表 C.3。

表 C.3 证书注销接口规范

功能简介	证书注销，根据证书相关信息注销证书。
接口名称	String certRevoke(String revokeParameter, StringsysCode)

表 C.3 证书注销接口规范（续）

参数说明	
入参说明	revokeParameter：注销证书内容以字符串方式，具体如下。 解密后的文件内容为： ——<CERTSN>证书序列号</CERTSN>，可选项 ——<KH>卡号</KH> ——<XZQHDM>发卡地区行政区划代码</XZQHDM> ——<REASON>注销原因，1=密钥泄露，4=被取代，5=停止使用，9=其他原因</REASON > sysCode：当前发起请求业务系统的系统代码 ID，通过协商后，统一规划的业务系统代码，必填项
返回值	返回一个字符串，内容解释如下。 <STATE>0 或 1</STATE> <ERRORCODE>1000</ERRORCODE> 标记说明： <STATE>操作状态：0=成功，1=失败 <ERRORCODE>错误代码

d)证书更新 certUpdate

证书更新接口规范见表 C.4。

表 C.4 证书更新接口规范

功能简介	证书更新，将原证书进行注销，并根据证书更新信息，重新签发新证书并返回。 以密文方式进行数据传输，加密方式请参考 GM/T 0010—2012《SM2 密码算法加密签名消息语法规范》9.1 数字信封章节。
接口名称	StringcertUpdate (String updateParameter String sysCode)
参数说明	
入参说明	updateParameter：证书更新申请以字符串方式，具体如下。 解密后的文件内容为： ——<XM>姓名</XM> ——<KH>卡号</KH> ——<SHBZHM>社会保障号码</SHBZHM> ——<QMGY>签名公钥</QMGY> ——<SF>算法</SF> ——<XZQHDM>发卡地区行政区划代码</XZQHDM> sysCode：当前发起请求业务系统的系统代码 ID，通过协商后，统一规划的业务系统代码，必填项

表 C.4 证书更新接口规范（续）

返回值	返回一个字符串，内容解释如下。 <STATE>0 或 1</STATE> <ERRORCODE>1000</ERRORCODE> <QMZS>签名证书</QMZS> <JMZS>加密证书</JMZS> <JMMY>加密密钥</JMMY> <ZKMY>主控密钥</ZKMY> <GLYPIN>管理员 PIN</GLYPIN> 标记说明： <STATE>操作状态：0=成功，1=失败 <ERRORCODE>错误代码 <QMZS>签名证书 <JMZS>加密证书 <JMMY>加密密钥密文 <ZKMY>主控密钥 <GLYPIN>管理员 PIN

e)证书挂失/解挂 certOper

证书挂失/解挂接口规范见表 C.5。

表 C.5 证书挂失/解挂接口规范

功能简介	证书挂失/解挂。 以密文方式进行数据传输，加密方式请参考 GM/T 0010—2012《SM2 密码算法加密签名消息语法规范》9.1 数字信封章节。
接口名称	String certOper(StringoperParameter, StringsysCode)
参数说明	
入参说明	operParameter：挂失证书内容以字符串方式，具体如下。 解密后的文件内容为： ——<CERTSN>证书序列号</CERTSN>，可选项 ——<KH>卡号</KH> ——<XZQHDM>发卡地区行政区划代码</XZQHDM> ——<OPERTYPE>操作类型：1=挂失，2=解挂</OPERTYPE> ——<REASON>挂失原因，1=密钥泄露，6=证书挂起，9=其他原因</REASON> sysCode：当前发起请求业务系统的系统代码 ID，通过协商后，统一规划的业务系统代码，必填项
返回值	返回一个字符串，内容解释如下。 <STATE>0 或 1</STATE> <ERRORCODE>1000</ERRORCODE> 标记说明：

	<STATE>操作状态：0=成功，1=失败 <ERRORCODE>错误代码

f)管理员 PIN 查询 certAdminPinQuery

管理员 PIN 查询接口规范见表 C.6。

表 C.6 管理员 PIN 查询接口规范

功能简介	管理员 PIN 查询。 以密文方式进行数据传输，加密方式请参考 GM/T 0010—2012《SM2 密码算法加密签名消息语法规范》9.1 数字信封章节。
接口名称	String certAdminPinQuery(String pinParameter; String sysCode)
参数说明	
入参说明	pinParameter 管理员 PIN 查询申请以字符串方式，具体如下。 解密后的文件内容为： ——<CERTSN>证书序列号</CERTSN > ——<KH>卡号</KH> ——<XZQHDM>发卡地区行政区划代码</XZQHDM> sysCode：当前发起请求业务系统的系统代码 ID，通过协商后，统一规划的业务系统代码，必填项
返回值	返回一个字符串，内容解释如下。 <STATE>0 或 1</STATE> <ERRORCODE>1000</ERRORCODE> <ZKMY>主控密钥</ZKMY> <GLYPIN>管理员 PIN</GLYPIN> 标记说明： <STATE>操作状态：0=成功，1=失败 <ERRORCODE>错误代码 <ZKMY>主控密钥 <GLYPIN>管理员 PIN

参考文献

[1] GB/T 31506—2022 信息安全技术 政务网站系统安全指南

[2] GB/T 35274—2017 信息安全技术 大数据服务安全能力要求

[3] GB/T 35295—2017 信息技术 大数据 术语

[4] GB/T 35589—2017 信息技术 大数据 技术参考模型

[5] GB/T 36073—2018 数据管理能力成熟度评估模型

[6] GB/T 42012—2022 信息安全技术 即时通信服务数据安全要求

[7] JR/T 0025—2018 中国金融集成电路（IC）卡规范

[8] JR/T 0055—2009 银行卡联网联合技术规范

[9] JR/T 0171—2020 个人金融信息保护技术规范

[10] 《人力资源社会保障部关于开展社会保障卡持卡人员基础信息库建设的通知》（人社部发〔2014〕36 号）

[11] 《中国人民银行办公厅 人力资源社会保障部办公厅关于印发具有金融功能的第三代社会保障卡技术规范的通知》（银办发〔2017〕170 号）

[12] 《关于印发社会保障卡读写终端接口规范的通知》（人社信息函〔2016〕38 号）

[13] 《关于印发<电子社会保障卡服务渠道管理办法（试行）>和<电子社会保障卡服务渠道接入安全技术规范（1.0 版）>的通知》（人社网信函〔2020〕22 号）