ICS 点击此处添加 ICS 号

点击此处添加中国标准文献分类号

DB11

北　京　市　地　方　标　准

DB XX/ XXXXX—XXXX

北京民生卡二维码技术规范

Technical specification for two-dimensional bar code of Beijing people's livehood card

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

北京市市场监督管理局　　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。

本文件由北京市经济和信息化局提出并归口。

本文件由北京市经济和信息化局组织实施。

本文件起草单位：北京市经济和信息化局、北京市大数据中心、北京市人力资源和社会保障局、北京金融大数据有限公司、中国银联股份有限公司北京分公司、北京市政交通一卡通公司、中电长城网际系统应用有限公司、北京思源政通科技集团有限公司、广东德生科技股份有限公司、厦门市美亚柏科信息股份有限公司、福建博思软件股份有限公司、首都信息发展股份有限公司、北京握奇数据股份有限公司、北京鲲鹏联合创新中心有限公司、航天科工二院智慧市政与安保科技中心、北京市民政局、北京市教育委员会、北京市残疾人联合会、北京市退役军人事务局、北京市卫生健康委员会、北京市园林绿化局、北京市医疗保障局、北京市自来水集团、国网北京市电力公司、北京市燃气集团有限责任公司。

本文件主要起草人：

北京民生卡二维码技术规范

1 范围

本文件规定了北京民生卡二维码的参考模型、数据结构、使用流程、接口以及其对移动应用程序、受理终端、安全的要求。

本文件适用于北京民生卡二维码应用建设运营单位对二维码的生成、使用及管理等，以及北京民生卡二维码相关业务系统、受理终端、移动应用程序等设计、研发与应用。

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 12905—2019 条码术语

GB/T 18284 快速响应矩阵码

GB/T 25069—2010 信息安全技术 术语

GB/T 27766 二维条码 网格矩阵码

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（所有部分） 信息安全技术 SM2椭圆曲线公钥密码算法

GB/T 36901—2018 电子证照 总体技术架构

3 术语和定义

下列术语和定义适用于本文件。

3.1

北京民生卡 beijing people's livehood card

依托第三代社会保障卡，整合社会保障、交通出行、医疗健康、养老助残、残疾人保障、公共缴费、公园景点、校园应用等民生应用而形成的具有金融功能的民生卡，包括北京民生卡实体卡和北京民生卡电子卡。

3.2

二维码 two-dimensional bar code

在两个维度方向上都表示信息的条码符号。

[来源:GB/T 12905—2019，2.3]

3.3

北京民生卡二维码 two-dimensional bar code of people's livehood card

根据北京民生卡二维码技术规范生成的二维码，支撑北京市各类民生应用，包括北京民生卡二维码（标准码）和北京民生卡二维码（简码）两种形式。

3.4

北京民生卡二维码（标准码）two-dimensional bar code of people's livehood card (standard code)

应用于同时支持在线和离线场景的北京民生卡二维码。

3.5

北京民生卡二维码（简码）two-dimensional bar code of people's livehood card (simplified code)

应用于身份服务和支付等在线场景的北京民生卡二维码，适用于不能识别复杂二维码的受理终端。

3.6

行业码 industry bar code

根据国家相关行业标准生成并应用在具体行业的条码。

3.7

发码平台 two-dimensional bar code publishing platform

实现北京民生卡二维码生成与解析、权益信息管理、支付订单管理、证书管理及风险控制等功能的信息系统。

3.8

统一支付系统 unified payment system

汇聚第三方支付渠道，提供统一的、多渠道的支付能力的信息系统。

3.9

统一权益信息共享应用平台 unified equity information sharing platform

自然人身份权益数据共享应用的信息系统。

3.10

受理终端 terminal

安装于受理点的用于与实体卡、二维码、人脸或其它方式配合共同完成身份认证、权益识别、交易等操作的设备。。

3.11

移动应用程序 mobile applications

移动终端上完成北京民生卡二维码和行业码相关业务处理的应用程序。

3.12

电子证照 electronic certificate

由计算机等电子设备形成、传输和存储的证照数据文件。

[来源:GB/T 36901—2018，3.3]

3.13

公钥 public key

在某一实体的非对称密钥对中，能够公开的密钥。

[来源:GB/T 25069—2010，2.2.2.43]

3.14

私钥 private key

一种用于控制密码变换操作（例如加密、解密、密码校验函数计算、签名生成或签名验证）的符号序列。

[来源:GB/T 25069—2010，2.2.2.106]

4 符号和缩略语

下列缩略语适用于本文件。

APP 应用程序（APPlication）

DPI 每英寸点数 （Dots Per Inch）

HTTP 超文本传输协议（HyperText Transport Protocal）

HTTPS 超文本传输安全协议（HyperText Transport Protocal over Secure sockets Layer）

JOSN JavaScript对象标记 (JavaScript Object Notation)

QR Code 快速响应矩阵码（Quick Response Code）

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 分组密码加密算法（SM4 Cryptographic Algorithm）

SSL/TLS 安全套接层/传输层安全 （Secure Sockets Layer/Transport Layer Security)

UTC 协调世界时 （Coordinated Universal Time）

5 北京民生卡二维码参考模型

5.1 业务应用场景

北京民生卡能够为用户提供多业务应用场景下的权益身份验证、证照核验和支付功能，服务于社会保障、交通出行、医疗健康、养老助残、残疾人保障、公共缴费、公园景点、校园应用等多种业务应用场景。典型业务应用场景见附录A。

北京民生卡包括实体卡和电子卡，每张北京民生卡实体卡均唯一对应一张电子卡。北京民生卡二维码为电子卡生成唯一二维码，同时也可为其他电子证照生成唯一二维码。

用户采用被扫模式使用北京民生卡二维码，由用户移动应用程序（APP）出示北京民生卡二维码，由受理终端进行扫码。

5.2 参考模型

基于角色和所支撑系统给出了北京民生卡二维码参考模型，如图1所示。

基础平台提供方：由多个机构担任，共同提供北京民生卡二维码各类应用共性所需的基础平台服务。基础平台包括但不限于发码平台、统一权益信息共享应用平台、统一支付系统等。

业务应用方：针对社会保障、交通出行、医疗健康、养老助残、残疾人保障、公共缴费、公园景点、校园应用等业务应用场景开展业务。业务应用方通过受理终端扫码并由业务系统进行相应的业务处理。

移动应用方：提供北京民生卡移动应用服务。移动应用方通过对接基础平台提供方提供的发码平台，以及业务应用方提供的受理终端和业务系统，为用户提供北京民生卡移动应用服务。

证书管理中心：为基础平台提供方、业务应用方和移动应用方提供北京民生卡二维码相关证书的生成、发放、验证、更新、注销等证书服务。

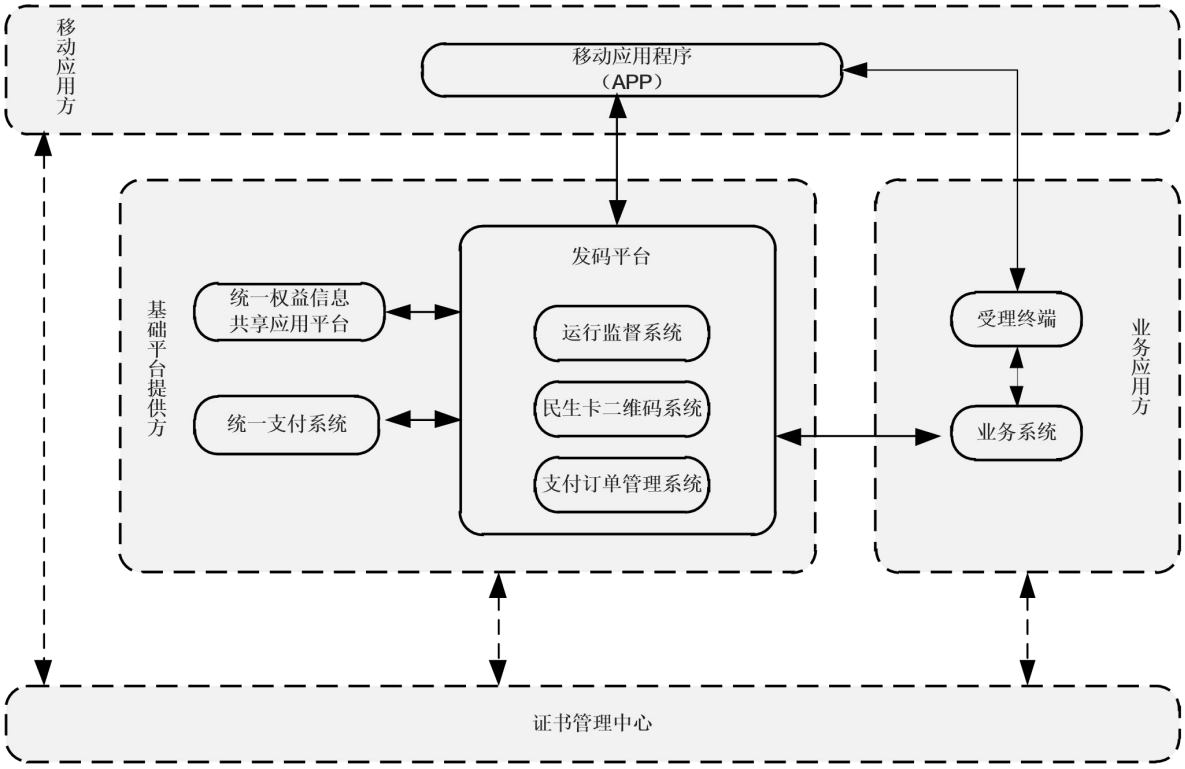

图 1　北京民生卡二维码参考模型

表1对北京民生卡参考模型中各系统主要功能进行了说明。

表 1　参考模型相关系统功能表

系统		功能描述
发码平台	民生卡二维码系统	负责北京民生卡二维码生成、解析、验证、管理以及行业码转发，并为业务系统提供二维码的管理服务。
	支付订单管理系统	负责对接“统一支付系统”和业务系统，实现支付请求的接收、拆分，调用“统一支付系统”进行费用支付，支付完成后同步支付结果。
	运行监控系统	负责对北京民生卡二维码和电子卡关联的服务使用情况以及使用安全进行监测管理。
统一权益信息共享应用平台		负责统一输出各类民生权益，当生成北京民生卡二维码时，为北京民生卡二维码系统提供权益状态信息。
统一支付系统		负责汇聚第三方支付渠道，提供统一的、多渠道的支付能力保障并进行支付管理。接收支付订单管理系统的支付请求，完成相关的业务费用支付，费用支付结束后向支付订单

	管理系统反馈支付信息和电子票据等，并提供对账功能等。
受理终端	负责对北京民生卡二维码进行扫描并识别二维码信息，对二维码进行有效性和安全性验证，识别后向业务系统传输二维码信息。
业务系统	负责进行相关业务办理，办理完成后向发码平台反馈业务办理相关信息。
移动应用程序（APP）	负责北京民生卡二维码和行业码相关业务处理，包括 APP 前端及后台。

6 北京民生卡二维码数据结构

6.1 北京民生卡二维码

北京民生卡二维码采用二进制（8bit-byte）编码方式。二维码采用Base64编码方式将字节数组编码后进行二维码图片转换，转换时应使用GB/T 18284或GB/T 27766确定的码制，通过移动应用程序（APP）进行展示。

为了适应不同应用环境的需要，北京民生卡二维码由北京民生卡二维码标准码和北京民生卡二维码简码两类组成。

6.2 北京民生卡二维码标准码

6.2.1 标准码数据结构

北京民生卡二维码（标准码）是同时支持在线和离线业务应用场景下身份认证、支付、证照出示和验证等业务的二维码结构。

北京民生卡二维码标准码由237-349字节长度组成，包含标准域、扩展域、安全域。北京民生卡二维码标准码数据结构如表2所示。

表 2 北京民生卡二维码标准码数据结构

信息域	编号	业务字段名称	字段代码	长度（字节）	字段业务作用
标准域（A 段）	1	码体系标识	TAG_CODE	4	指示此码是否属于北京城市码体系
	2	码授权标识	TAG_SOURCE	4	指示此码由哪个授权出码单位发出
	3	码属性标识	TAG_TYPE	4	指示码的类型
	4	码身份标识类型	TAG_PID_TYPE	2	指个人身份标识的类型
	5	码身份标识长度	TAG_PID_LEN	1	个人身份标识编码的长度
	6	码身份标识	TAG_PID	12	个人身份标识编码
扩展域（E 段）	7	扩展域长度	BUS_DATA_LEN	1	与业务相关的属性信息的长度，7-13 项内容长度
	8	用户权益数量	CERT_USER_RIGHT_COUNT	1	表示用户权益的数量

	9	用户权益标识	CERT_USER_RIGHT	0-40	每项权益用两个字节标识，权益标识与统一权益信息共享应用平台的权益信息建立一一映射关系。
	10	业务应用场景标识	CERT_SCENE	4	用户开通的业务应用场景标识，参见附录 B。
	11	支付方式	BUS_PAY_CHN	1	记录当前用户支付方式。用户第一次使用支付时，需要与北京民生卡进行绑定进行支付。
	12	免密支付限额	BUS_PAY_LIM	1	二维码免密支付的金额上限。
	13	扩展信息	BUS_EXT	0-72	由具体应用或业务定义的其他扩展信息
安全域（S 段）	14	码体生成时间	SCU_CTIME	4	二维码串生成时间，精确到秒
	15	码体有效时长	SCU_DURA	4	二维码串有效时长，精确到秒
	16	码体验签方式	SCU_SIGN_TYPE	1	使用发码机构公钥做一次验签，或发码机构公钥和用户证书公钥两次验签
	17	用户证书公钥	CERT_USER_PUB	33	用户公钥，使用 SM2 算法生成的非对称密钥对
	18	用户证书生成时间	CERT_DURA	4	证书生成时间，精确到秒
	19	用户证书有效时长	CERT_DURA	4	证书有效时长，精确到秒
	20	用户证书签名	CERT_SIGN	72	使用机构的私钥对用户证书进行签名值，使用 SM2 算法对第 4、6、17、18、19 项进行签名
	21	机构证书编号	DEPT_CERT_NUMBER	4	发放用户证书的机构证书编号
	22	码体签名数据	SCU_SIGN	72	使用用户私钥对 1-21、23 项进行签名
	23	码版本标识	TAG_VERSION	4	指示此码的生成规则和版本，兼容不同版本的码规则

北京民生卡二维码的扩展信息根据实际业务应用场景定义扩展域值数据，扩展信息数据结构如表3所示。

表 3　扩展信息数据结构

序号	数据元	长度（字节）	备注
1	扩展域类型标识	1	
2	扩展域值	0-71	

6.2.2　电子证照扩展信息

北京民生卡电子卡作为电子证照类型之一，可以直接用北京民生卡二维码标准码生成该电子证照二维码，并用于证照出示及证照核验，无需用到“扩展信息”；当使用北京民生卡二维码标准码生成其他类型电子证照二维码时，需通过使用“扩展信息”数据结构来进行电子证照的出示和核验，扩展信息数据结构如表4所示。

表 4　电子证照扩展信息数据结构

序号	数据元	长度（字节）	备注
1	扩展域类型标识	1	值为 1，表示扩展类型为电子证照
2	证照类型	2	表示电子证照类型
3	证照编号	0-69	表示电子证照编号

6.3　北京民生卡二维码简码

北京民生卡二维码（简码）是基于用户身份权益的服务和支付等业务简单的在线业务应用场景构建的二维码结构，北京民生卡二维码简码结构设计将参照现有主流二维码标准，支持主流支付渠道扫码设备，总长度不超过19个纯数字。

表 5　北京民生卡二维码简码数据结构

信息域	序号	数据元	长度 （字节）	字段业务作用
码体标准域	1	码体系标识	2	固定值：表示北京城市码体系
	2	码属性标识	2	固定值：表示属于城市码“个人码”
	3	码授权标识	4	固定值：表示被授权发码单位
	4	码身份标识	11	用户身份标识，指向用户唯一身份标识信息。

7　北京民生卡二维码使用流程

7.1　北京民生卡二维码生成流程

7.1.1　二维码生成网络环境

北京民生卡二维码生成流程分为在线流程及离线流程，在线流程是用户移动应用程序（APP）具备网络环境时，生成北京民生卡二维码的流程，离线码流程是用户移动应用程序（APP）不具备网络环境时，生成北京民生卡二维码的流程，在线及离线流程生成结果均为北京民生卡二维码。标准码生成支持离线及在线环境，简码生成支持在线环境。

7.1.2　在线生成简码

在线生成简码流程见图2，具体在线生成简码流程描述如下：

a)　用户在 APP 端发起二维码申请；
b)　APP 后台根据注册信息进行用户身份校验；
c)　北京民生卡二维码系统获取二维码风控指标；
d)　向统一权益信息共享应用平台发送获取用户权益信息请求，统一权益信息共享应用平台收到请求后，向北京民生卡二维码系统提供用户权益信息；

e） 北京民生卡二维码系统进行二维码数据生成，并将二维码数据传送给 APP 后台；
f） 由 APP 端进行二维码展示；
g） 简码支持条形码展示。

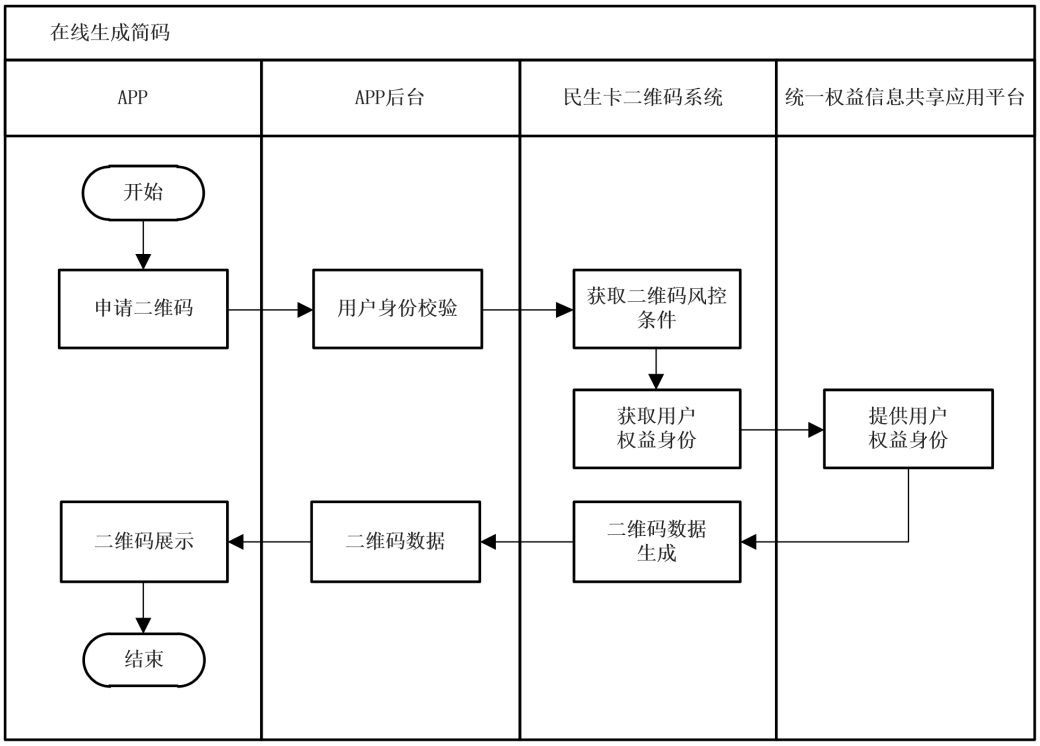

图 2　在线生成简码流程

7.1.3　在线生成标准码

在线生成标准码流程见图3，具体在线生成标准码流程描述如下：

a） 用户在 APP 端发起二维码相关数据申请；
b） APP 后台根据注册信息进行用户身份校验并请求二维码相关数据；
c） 北京民生卡二维码系统获取用户和机构证书信息、二维码风控条件；
d） 向统一权益信息共享应用平台发获取用户权益信息请求，统一权益信息共享应用平台收到请求后，向北京民生卡二维码系统提供用户权益信息信息；
e） 北京民生卡二维码系统生成二维码相关数据，并将这些数据传送给 APP 后台；
f） APP 前端根据 APP 后台传过来的二维码相关数据生成并展示二维码。

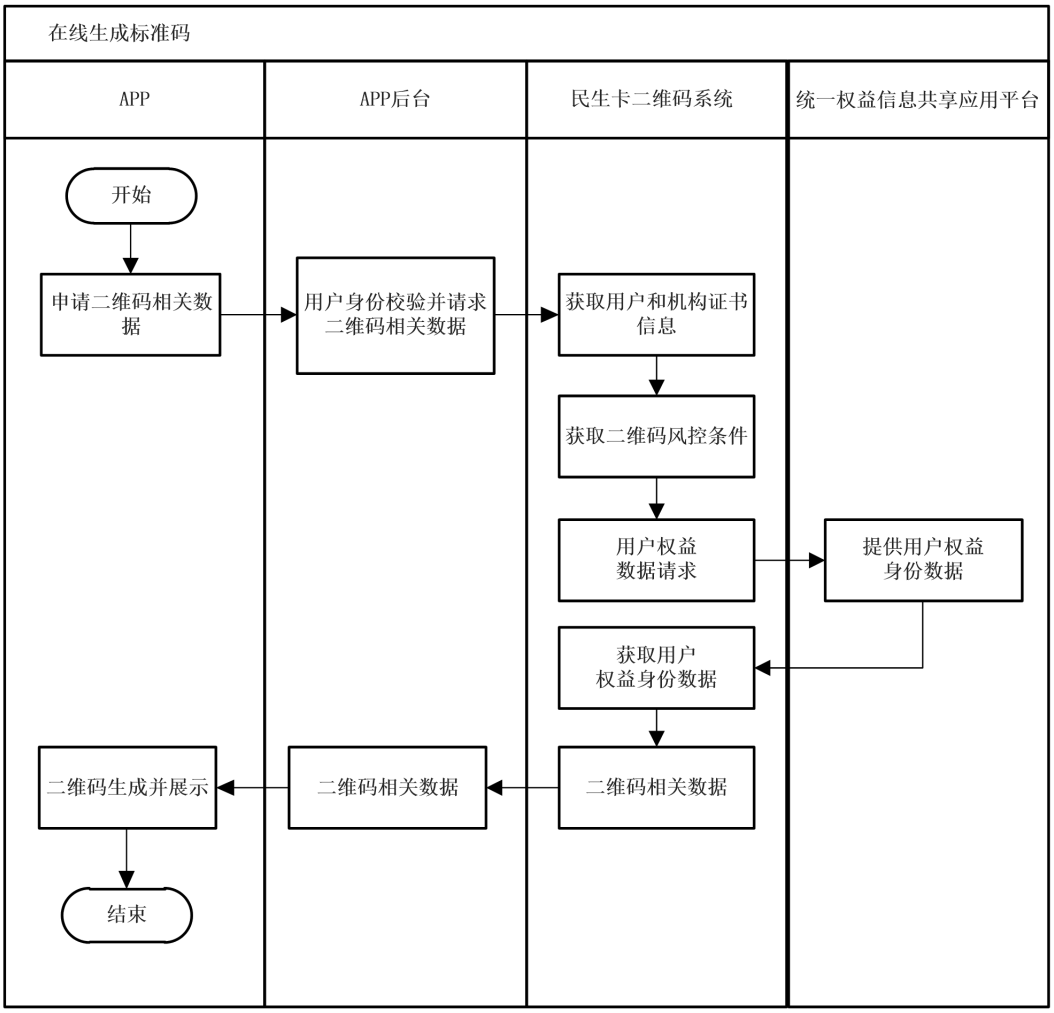

图 3　在线生成标准码流程

7.1.4　离线生成标准码

离线生成标准码流程见图4，具体离线生成标准码流程描述如下：

a)　离线生成标准码需在用户在线时提前向北京民生卡二维码系统获取二维码生成相关数据，包括机构证书签名、二维码风控条件、权益信息等，在本地更新并进行存储。

b)　当处于离线状态时，用户在 APP 端申请二维码，APP 前端基于在线时获取的二维码相关数据生成二维码并展示。

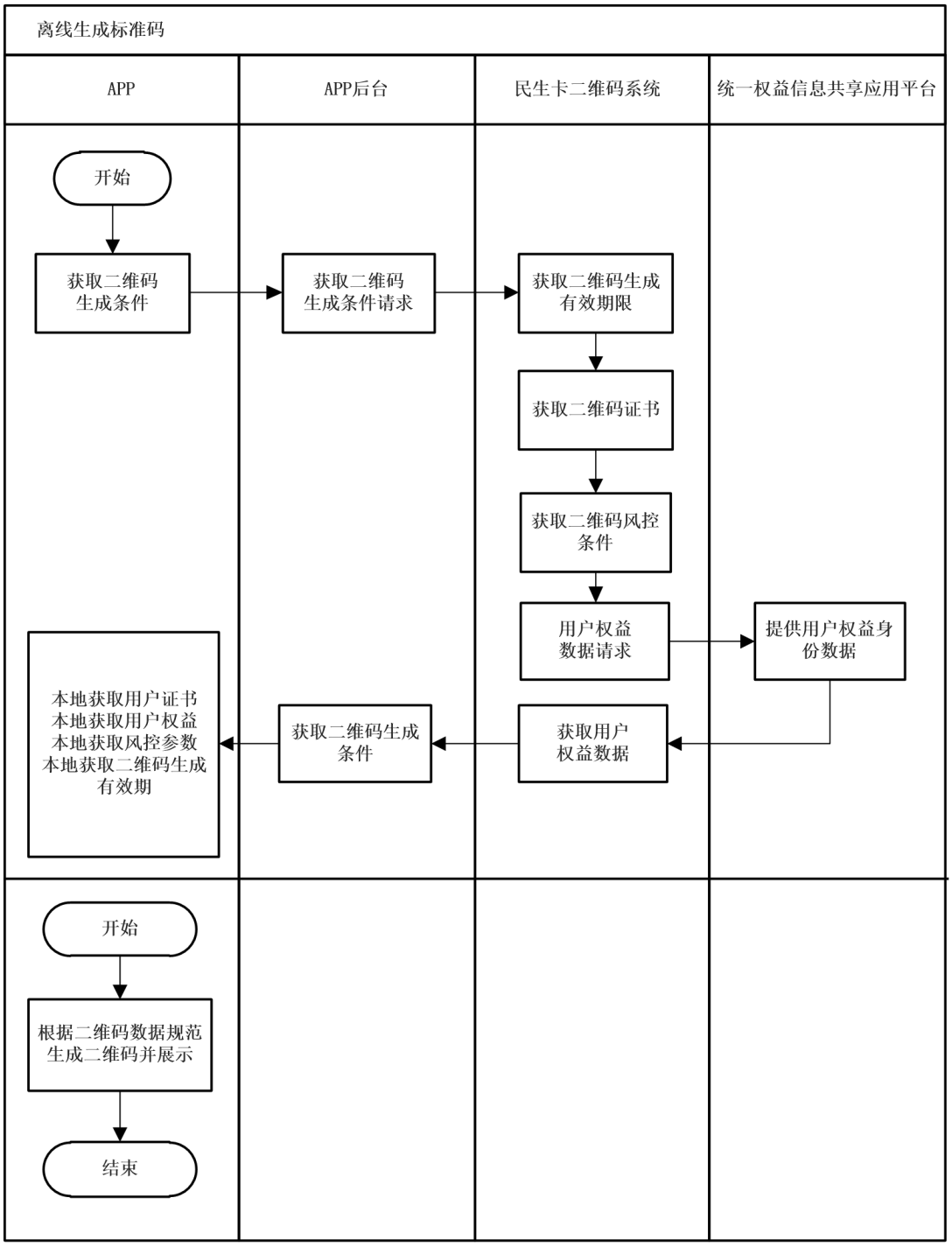

图 4　离线生成标准码流程

7.2　北京民生卡二维码（标准码）安全核验流程

用户通过移动应用程序（APP）展示北京民生卡二维码（标准码）后，需要受理终端对北京民生卡二维码进行扫描、信息识别及签名验证。北京民生卡二维码（标准码）验证签名流程是身份认证流程、证照出示核验流程及支付流程的重要节点。北京民生卡二维码验证签名支持离线验证签名及在线验证签名。受理终端将对北京民生卡二维码签名及其时效性做验证，保证北京民生卡二维码的有效性。

安全核验流程见图5，具体的安全核验流程描述如下：

a) 终端初始化时，证书管理中心将机构证书公钥同步到受理终端；受理终端存储机构证书公钥，具备二维码解析、验证能力；

b) 用户出示二维码，受理终端进行二维码扫描，识别二维码信息；

c) 受理终端进行二维码校验：

1) 验证二维码有效期；

2) 验证用户证书有效期；

3) 基于发码机构证书公钥验证机构证书签名有效性；

4) 验证码体数据签名。

d) 当验证签名（离线/在线）时，受理终端用证书管理中心的公钥验证签名；

e) 若验证失败，则服务结束，验证通过后，将数据发送到业务系统及北京民生卡二维码系统。

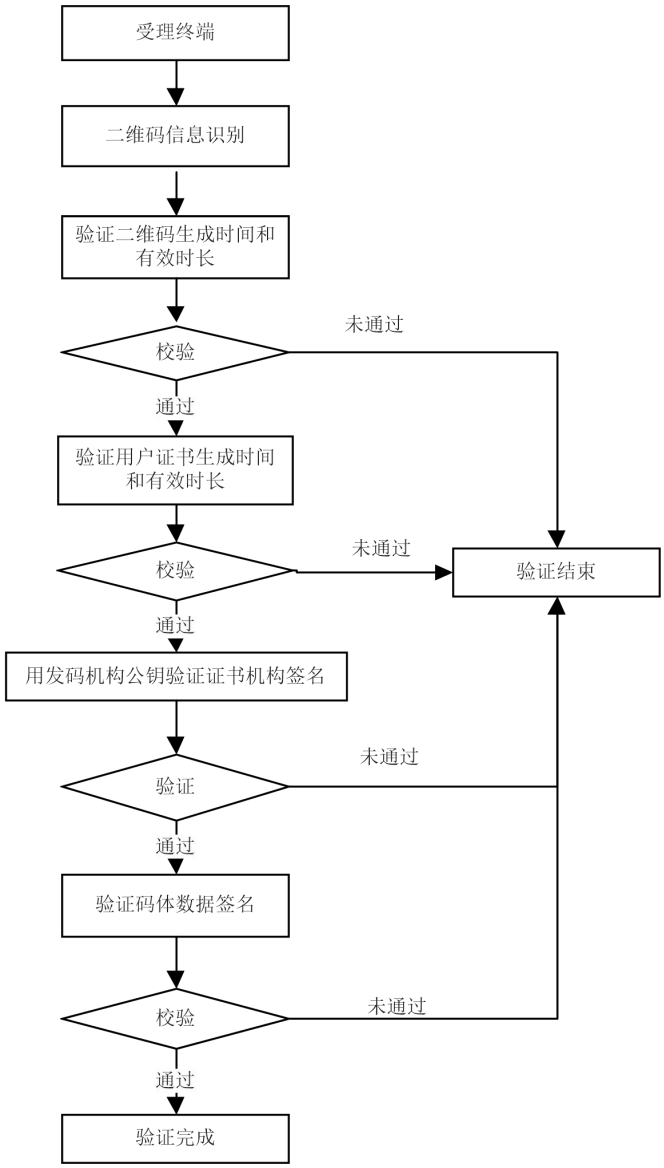

图 5　安全核验流程

7.3　身份认证流程

7.3.1 在线身份认证（标准码、简码）

在线身份认证流程见图 6，具体在线身份认证流程描述如下：

a) 用户通过 APP 展示二维码；
a) 受理终端进行二维码扫描，识别二维码信息，将二维码信息发送到业务系统；
b) 业务系统二维码信息发送到北京民生卡二维码系统；
c) 北京民生卡二维码系统接收到二维码信息后进行解析，将解析后用户身份信息发送到业务系统；
d) 业务系统进行业务办理。

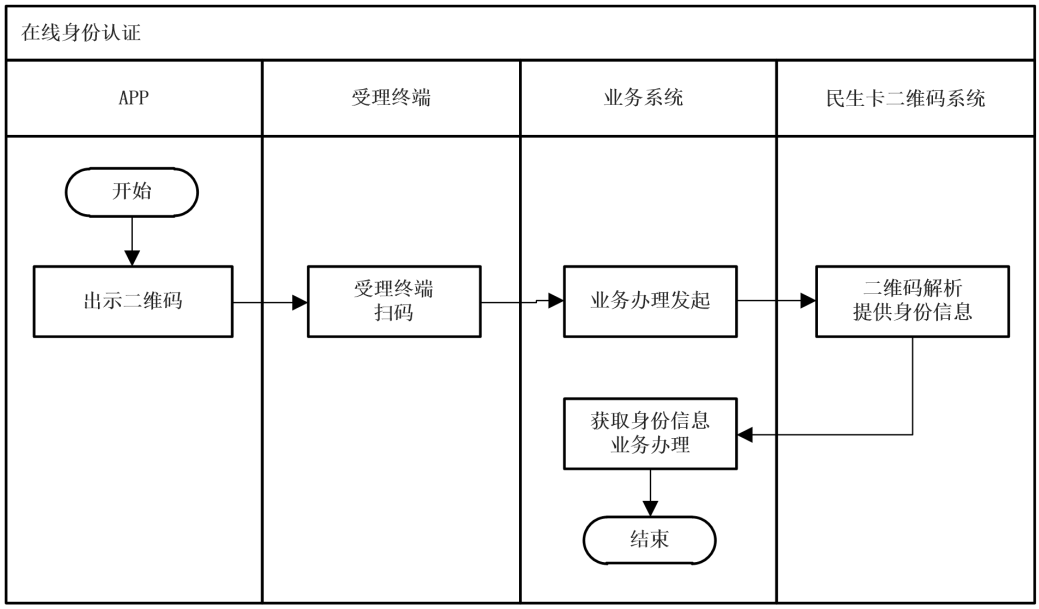

图 6 在线身份认证流程

7.3.2 离线身份认证（标准码）

离线身份认证（标准码）的流程见图7，具体离线身份认证（标准码）的流程描述如下：

a) 用户通过 APP 展示二维码；
b) 受理终端进行二维码扫描，判断二维码有效性并识别二维码信息；
c) 当具备网络环境时，将二维码信息发送到业务系统；
d) 业务系统二维码信息发送到北京民生卡二维码系统；
e) 北京民生卡二维码系统接收到二维码信息后进行解析，将解析后用户身份信息发送到业务系统；
f) 业务系统进行业务办理。

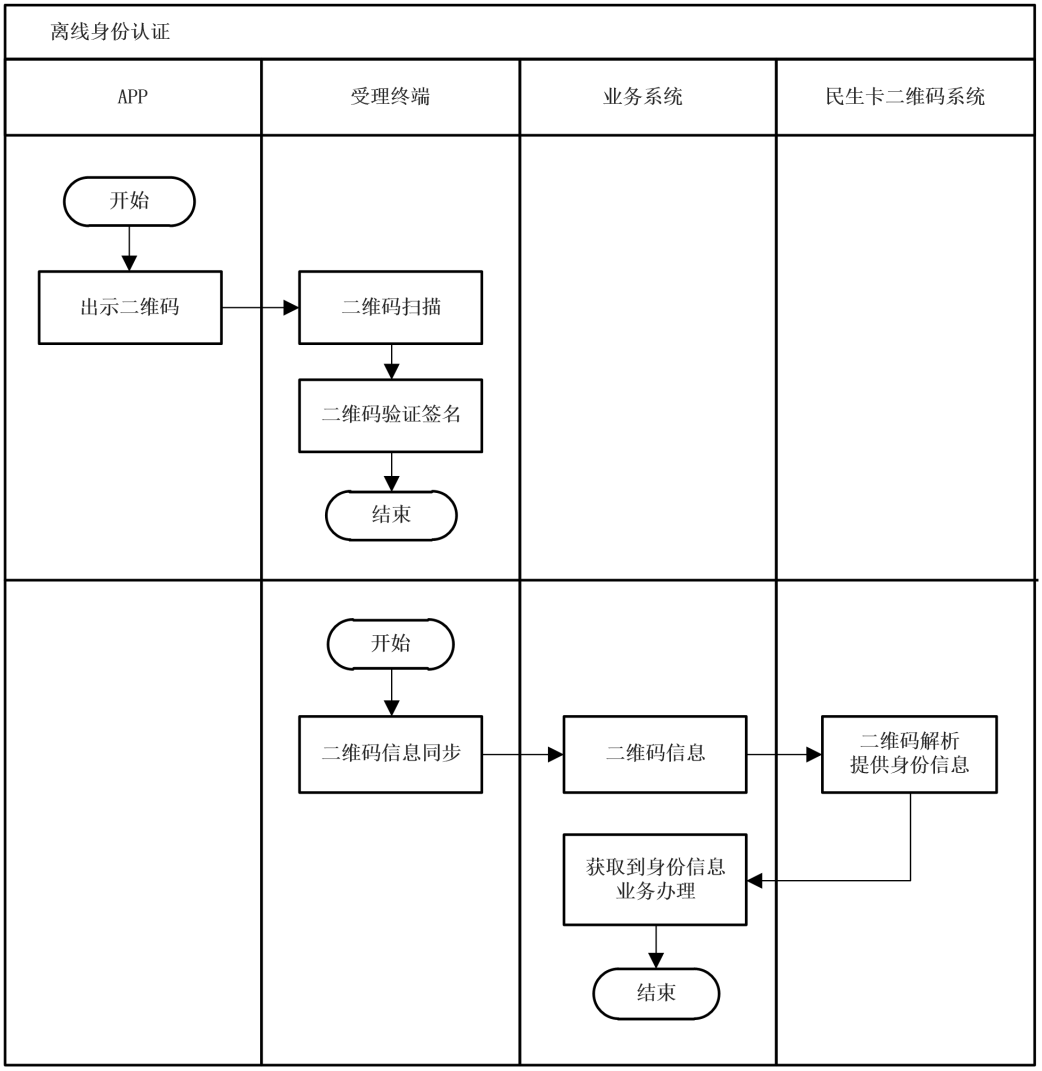

图 7　离线身份认证（标准码）流程

7.4　证照出示核验流程

7.4.1　电子证照二维码

电子证照是指由各单位依法出具的、具有法律效力的各类证照，电子证照二维码是基于电子证照信息生成的二维码，电子证照二维码更便于证照信息的快速读取。证照出示核验的电子证照源使用同一个电子证照系统，用户通过手机端APP展示电子证照的同时，可展示该电子证照相关联的电子证照二维码，业务系统通过二维码识别用户证照信息，判断证照信息的真伪性。证照出示核验使用二维码标准码生成，流程需要网络环境支持。

7.4.2　出示证照流程

出示证照流程见图8，具体出示证照流程描述如下：

a)　用户在 APP 端选择需要展示的证照；

b)　APP 后台将电子证照数据（身份信息、证照编号、证照类型）发送到北京民生卡二维码系统；

c)　由北京民生卡二维码系统生成包括证照信息及身份信息的二维码数据，推送到 APP 后台；

d)　APP 后台将二维码数据及电子证照推送到 APP 端；

e） APP 端进行二维码及证照展示。

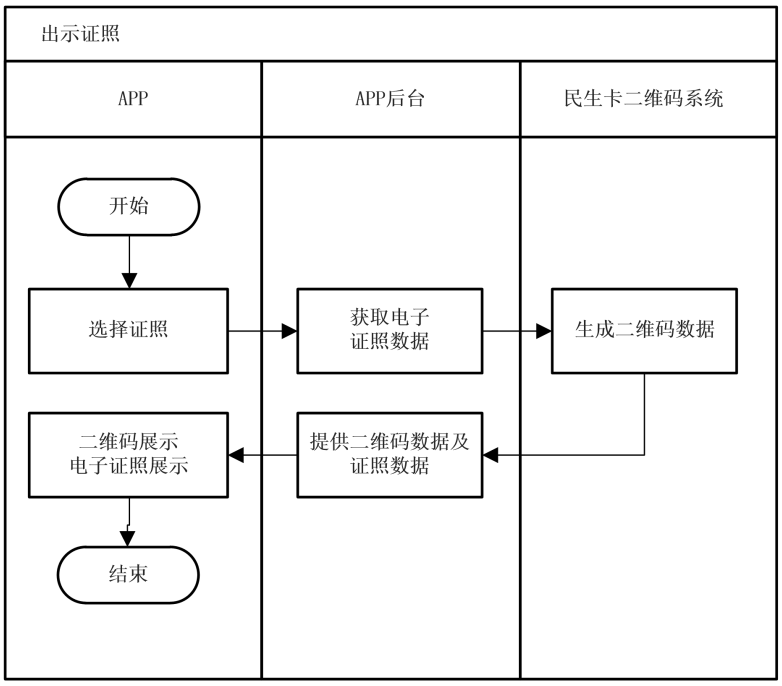

图 8　出示证照流程

7.4.3　证照核验流程

证照核验流程见图9，具体证照核验流程描述如下：

a） 用户通过移动应用程序（APP）展示电子证照及北京民生卡二维码；

b） 受理终端进行二维码扫描识别二维码信息，将二维码信息发送到业务系统，业务系统推送到北京民生卡二维码系统；

c） 北京民生卡二维码系统对二维码信息进行解析，将解析后的个人身份信息、证照类型、证照编号数据推送给业务系统；

d） 业务系统根据个人身份信息、证照类型、证照编号获取指定证照，获取电子证照后在业务系统及（或）受理终端进行展示；

e） 由人工进行电子证照核对。

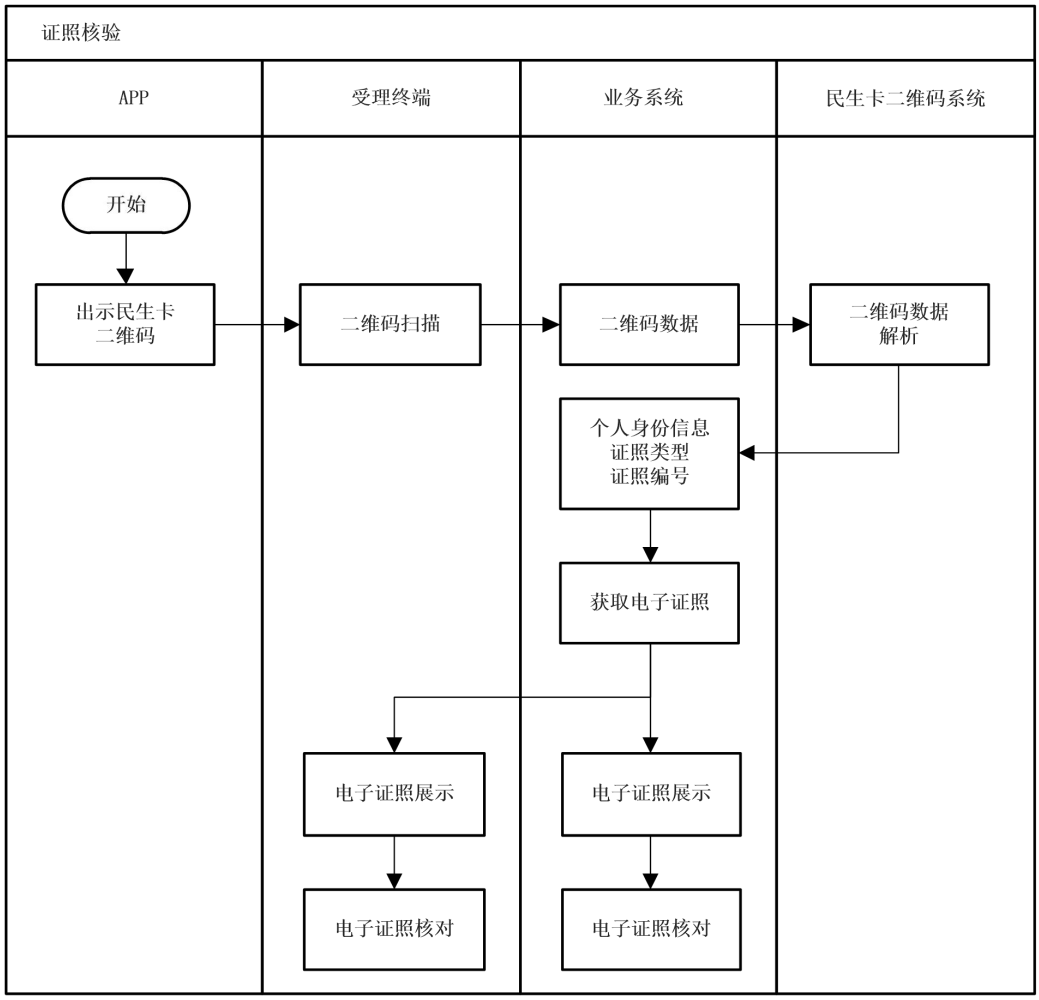

图 9　验证流程

7.5　支付流程

7.5.1　基于身份权益的费用支付

基于身份权益的支付流程见图10，具体基于身份权益的支付流程描述如下：

a)　用户在 APP 端展示二维码；

b)　受理终端进行二维码扫描并识别二维码信息，将二维码信息发送到业务系统；

c)　受理终端将二维码数据通过业务系统发送到北京民生卡二维码系统，同时业务系统开始业务办理；

d)　北京民生卡二维码系统将二维码数据进行解析后，发送到业务系统，业务系统进行业务计费并生成账单，向支付订单管理系统发送扣款请求（如需用户确认扣款，生成账单后发送到 APP，用户确认扣款后由支付订单管理系统向统一支付系统发送扣款请求）；

e)　支付订单管理系统接到扣款请求后，根据二维码支付渠道和绑定的支付方式生成交易扣款订单，用户确认支付，向统一支付系统进行扣款申请；

f)　统一支付系统接收扣款申请后调取外部支付渠道进行扣款，扣款完成后与支付渠道异步确认结果，并向支付订单管理系统同步扣款结果数据；

g)　支付订单管理系统将扣款结果数据同步到业务系统及受理终端，并向 APP 端推送扣款通知。

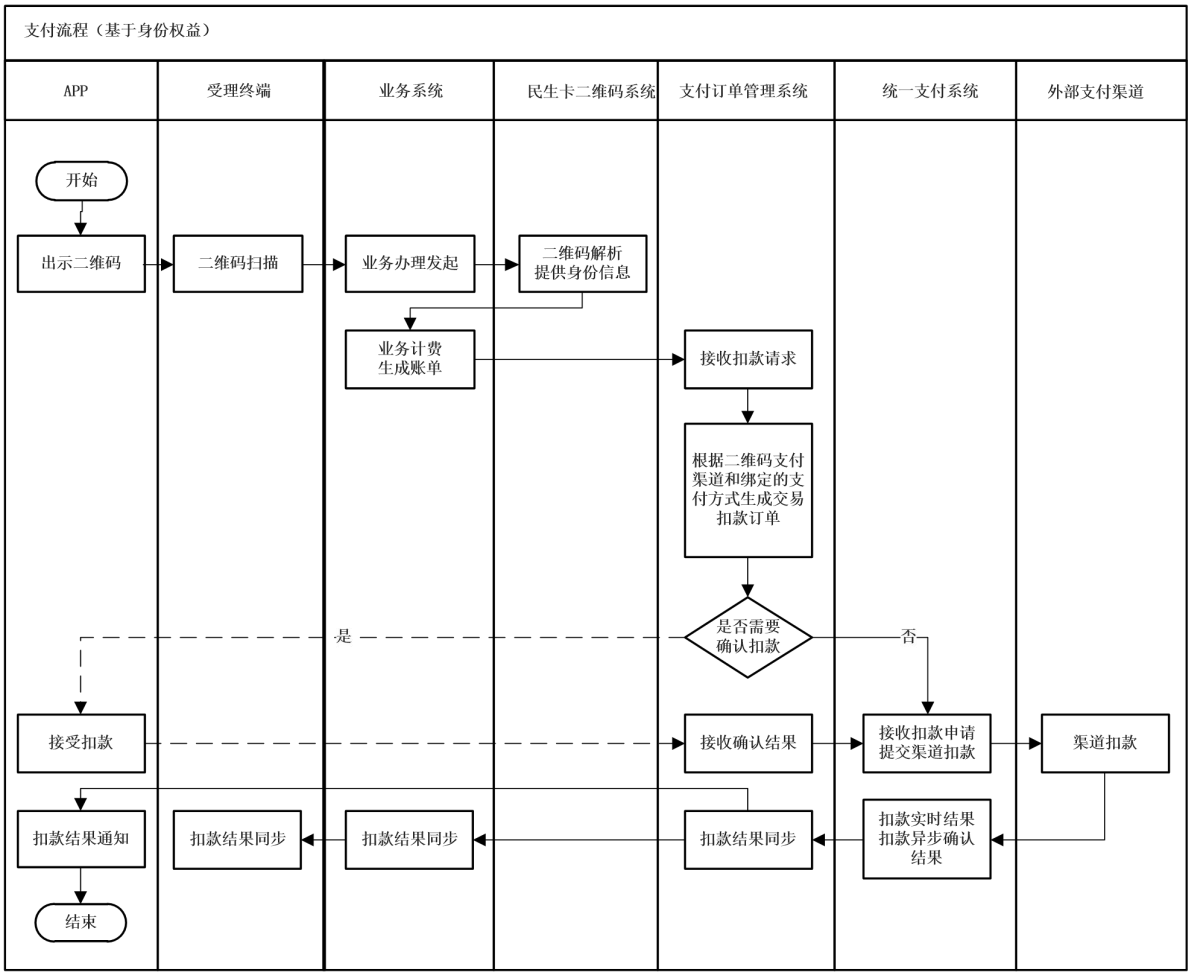

图 10　支付流程

7.5.2　无身份权益费用支付

无身份权益的支付主要用于无需身份权益的金融支付等业务应用场景使用，无身份权益的支付流程见图11，具体无身份权益的支付流程描述如下：

a）　用户在 APP 端展示二维码；

b）　受理终端进行二维码扫描，判断二维码有效性并识别二维码信息，将二维码信息发送到业务系统；

c）　业务系统将二维码信息和支付订单信息转发至支付订单管理系统；

d）　支付订单管理系统接到扣款请求后，根据二维码支付渠道和绑定的支付方式生成交易扣款订单，用户选择支付渠道并确认后，向统一支付系统进行扣款申请（如需用户确认扣款，用户确认支付渠道后进行扣款确认，用户确认扣款后由支付订单管理系统向统一支付系统发送扣款请求）；

e）　统一支付系统接收扣款申请后在 APP 端取得用户支付确认后，调取外部支付渠道进行扣款，扣款完成后与支付渠道异步确认结果，并向支付订单管理系统同步扣款结果数据；

f）　支付订单管理系统将扣款结果数据同步到业务系统及受理终端，并向 APP 端推送扣款通知。

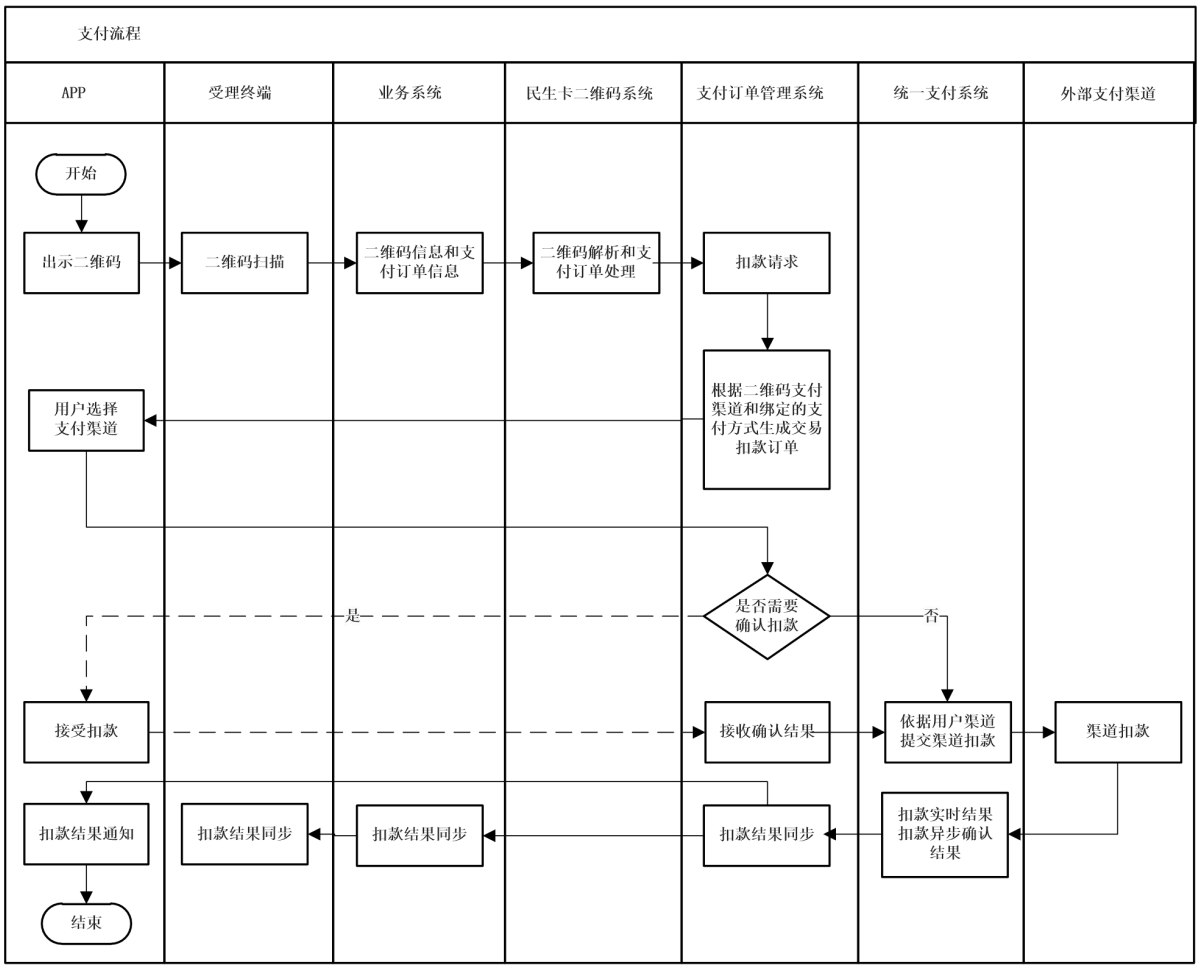

图 11　支付流程

8　北京民生卡二维码接口

8.1　总体要求

北京民生卡二维码接口通过HTTPS使用POST方法发送请求并进行响应，使用JSON进行数据交互。

8.2　激活业务应用场景

用于用户主动激活使用二维码的业务应用场景。详见表6、表7、表8。

表 6　激活业务应用场景接口说明

接口调用地址	activateTDCode
接口提供者	发码平台
接口消费者	移动应用程序（APP）后台
功能描述	激活使用二维码的业务应用场景

表 7　激活业务应用场景请求参数

序号	参数名称	参数	参数类型	必填	说明	示例值
1	应用 ID	appId	string	Y	移动应用程序 (APP) id	
2	业务参数	Data	string	Y	JSON 格式的业务数据	
3	应用签名	appSign	string	Y	签名值（由平台提供给应用的 AppSecret 用 SM4 进行对称加密算法签名）	
data 说明						
1	公钥	publicKey	string	Y	用户完成认证后，平台下发给用户的公钥，算法采用 SM2 非对称加密算法	
2	场景编号	sceneCode	string	Y	发码平台约定的特定应用场景的编号	

表 8　激活业务应用场景输出参数

序号	参数名称	参数	类型	说明	示例值
1	返回码	Code	string	01 代表成功	01
2	返回消息	Message	string	code = 01，message=”成功”， code = 其他，message=具体错误消息	
3	返回数据	Data	string		
data 数据结构定义					
1	版本信息	Version	string		
2	机构证书公钥	orgPublicKey	string		
3	证书类型	certType	string	01：用户证书　02：应用证书	
4	用户身份公钥	publicKey	string	由发码平台下发的用户公钥	
5	用户身份证书失效时间	invalidTime	datetime	证书失效时间。该值为 4 字节无符号整形数字。时间戳为从 UTC-8	

序号	参数名称	参数	类型	说明	示例值
				时区的 2020 年 1 月 1 日 0 时 0 分 0 秒起流逝的秒数。	
6	用户身份唯一标识	userId	string	由发码平台生成的唯一用户标识	
7	业务应用场景标识	Scene	string	用户已经申请开通的业务应用场景标识，共 4 个字节，32bit 位，对多代表 32 个场景。	
8	用户身份标签	userRight	string	用户拥有的权益	
9	证书机构签名	depSign	string	通过机构私钥采用SM2对3-8签名	
10	证书平台签名	Sign	string	通过平台私钥采用SM2对1-9签名	

8.3 获取用户证书

用于移动应用程序（APP）后台服务向发码平台获取生成二维码的用户证书。详见表9、表10、表11。

表 9 获取用户证书接口参数

接口调用	getCert
接口提供者	发码平台
接口消费者	移动应用程序（APP）后台服务
功能描述	APP 后台调用发码平台，获取用户身份证书，用于 APP 前端离线生成二维码。

表 10 获取用户证书请求参数

序号	参数名称	参数	参数类型	必填	说明	示例值
1	应用 ID	appId	string	Y	由发码平台提供的业务接入服务的标识 Id	101
2	业务参数	Data	string	Y	JSON 格式的业务数据	
3	应用签名	appSign	string	Y	签名值（由平台提供给应用的 AppSecret 用 SM4 进行对称加密算法签名）	
data 说明						
1	公钥	publicKey	string	Y	用户完成认证后，平台	

序号	参数名称	参数	参数类型	必填	说明	示例值
					下发给用户的公钥，算法采用SM2非对称加密算法	

表 11　获取标准码输出参数

序号	参数名称	参数	类型	说明	示例值
1	返回码	Code	string	01 代表成功	01
2	返回消息	Message	string	code = 01，message=”成功”， code = 其他，message=具体错误消息	
3	返回数据	Data	string	JSON 格式数据	
data 数据结构定义					
1	版本信息	Version	string		
2	机构证书公钥	orgPublicKey	string		
3	证书类型	certType	string	01：用户证书　02：应用证书	
4	用户身份公钥	publicKey	string	由发码平台下发的用户公钥	
5	用户身份证书失效时间	invalidTime	datetime	证书失效时间。该值为 4 字节无符号整形数字。时间戳为从 UTC-8 时区的 2020 年 1 月 1 日 0 时 0 分 0 秒起流逝的秒数。	
6	用户身份唯一标识	userId	string	由发码平台生成的唯一用户标识	
7	业务应用场景标识	Scene	string	用户已经申请开通的业务应用场景标识，共 4 个字节，32bit 位，最多代表 32 个场景。	
8	用户权益标签	userRight	string	用户拥有的权益	
9	证书机构签名	deptSign	string	通过机构私钥采用SM2对3-8签名	
10	证书平台签名	Sign	string	通过平台私钥采用SM2对1-9签名	

8.4 获取二维码标准码

移动应用程序（APP）后台服务向发码平台拉取二维码标准码信息。详见表12、表13、表14。

表 12 获取二维码标准码接口说明

接口调用	getStdTDCode
接口提供者	发码平台
接口消费者	移动应用程序（APP）业务后台
功能描述	获取二维码标准码

表 13 获取二维码标准码请求参数

序号	参数名称	参数	参数类型	必填	说明	示例值
1	应用 ID	appId	string	Y	由发码平台提供的业务接入服务的标识 Id	
2	业务参数	Data	string	Y	JSON 格式的业务数据	
3	应用签名	appSign	string	Y	签名值（由平台提供给应用的 AppSecret 用 SM4 进行对称加密算法签名）	
data 说明						
1	公钥	publicKey	string	Y	用户完成认证后，平台下发给用户的公钥，算法采用 SM2 非对称加密算法	

表 14 获取二维码标准码输出参数

序号	参数名称	参数	类型	说明	示例值
1	返回码	Code	string	01 代表成功	01
2	返回消息	Message	string	code = 01，message=”成功”， code = 其他，message=具体错误消息	
3	返回数据	Data	string		
data 数据结构定义					
1	二维码串	Tdcode	string	二维码标准码	

8.5 获取证照二维码

移动应用程序（APP）后台服务向发码平台拉取证照二维码信息。详见表15、表16、表17。

表 15 获取证照二维码接口说明

接口调用	getCertTDCode
接口提供者	发码平台
接口消费者	移动应用程序（APP）业务后台
功能描述	获取证照二维码（二维码标准码）

表 16 获取证照二维码请求参数

序号	参数名称	参数	参数类型	必填	说明	示例值
1	应用 ID	appId	string	Y	由发码平台提供的业务接入服务的标识 Id	
2	业务参数	Data	string	Y	JSON 格式的业务数据	
3	应用签名	appSign	string	Y	签名值（由平台提供给应用的 AppSecret 用 SM4 进行对称加密算法签名）	
data 说明						
1	公钥	publicKey	string	Y	用户完成认证后，平台下发给用户的公钥，算法采用 SM2 非对称加密算法	
2	用户证书类型	userCertType	string	N		
	用户证书编号	userCertCode	string	Y		

表 17 获取证照二维码输出参数

序号	参数名称	参数	类型	说明	示例值
1	返回码	Code	string	01 代表成功	01
2	返回消息	Message	string	code = 01，message=”成功”， code = 其他，message=具体错误	

序号	参数名称	参数	类型	说明	示例值
				消息	
3	返回数据	Data	string		
data 数据结构定义					
1	二维码串	Tdcode	string	二维码标准码	

8.6 获取二维码简码

移动应用程序（APP）后台服务向发码平台拉取二维码简码信息。详见表18、表19、表20。

表 18 获取二维码简码接口说明

接口调用	getSimTDCode
接口提供者	发码平台
接口消费者	移动应用程序（APP）业务后台
功能描述	获取二维码简码

表 19 获取二维码简码请求参数

序号	参数名称	参数	参数类型	必填	说明	示例值
1	应用 ID	appId	string	Y	由发码平台提供的业务接入服务的标识 Id	
2	业务参数	Data	string	Y	JSON 格式的业务数据	
3	应用签名	appSign	string	Y	签名值（由平台提供给应用的 AppSecret 用 SM4 进行对称加密算法签名）	
data 说明						
1	公钥	publicKey	string	Y	用户完成认证后，平台下发给用户的公钥，算法采用 SM2 非对称加密算法	

表 20 获取二维码简码输出参数

序号	参数名称	参数	类型	说明	示例值
1	返回码	code	string	01 代表成功	01
2	返回消息	message	string	code = 01，message=”成功”，	

序号	参数名称	参数	类型	说明	示例值
				code = 其他, message=具体错误消息	
3	返回数据	data	string		
data 数据结构定义					
1	二维码串	tdcode	string	二维码简码	

8.7 二维码解析

解析二维码信息，并返回解析结果。详见表21、表22、表23。

表 21 二维码解析接口说明

接口调用地址	getTDCodeInfo
接口提供者	发码平台
接口消费者	业务系统
功能描述	业务平台解析二维码

表 22 二维码解析请求参数

序号	参数名称	参数	参数类型	必填	说明	示例值
1	应用 ID	appId	string	Y	业务系统 id	
2	业务参数	data	string	Y	JSON 格式的业务数据	
3	应用签名	appSign	string	Y	签名值（由平台提供给应用的 AppSecret 用 SM4 进行对称加密算法签名）	
data 说明						
1	二维码字符串	tdcode	string	Y		

表 23 二维码解析输出参数

序号	参数名称	参数	类型	说明	示例值
1	返回码	code	string	01 代表成功	01
2	返回消息	message	string	code = 01，message=”成功”， code = 其他, message=具体错误	

序号	参数名称	参数	类型	说明	示例值
				消息	
3	返回数据	data	string		
data 数据结构定义					
1	用户唯一标识	userId	string		
2	用户姓名	userName	string		
3	用户身份类型	identityType	string	例如：身份证、北京通	
4	用户身份编号	identityCode	string	例如：身份证号、北京通号	
5	用户证照类型	certType	string	例如：医保卡，身份二维码和支付二维码这两个字段没值	
6	用户证照编号	certCode	string	例如：医保卡号，身份二维码和支付二维码这两个字段没值	
7	用户权益列表	userRights	List	<权益编码，权益名称>的数组	

8.8 提交支付订单

业务系统将支付请求提交到发码平台。详见表24、表25、表26。

表 24 提交支付订单接口说明

接口调用地址	orderCommit
接口提供者	发码平台
接口消费者	业务系统
功能描述	业务系统提交支付订单

表 25 提交支付订单请求参数

序号	参数名称	参数	参数类型	必填	说明	示例值
1	应用 ID	appId	string	Y	业务系统 id	
3	业务参数	data	string	Y	JSON 格式的业务数据	

序号	参数名称	参数	参数类型	必填	说明	示例值
4	应用签名	appSign	string	Y	签名值（由平台提供给应用的 AppSecret 用 SM4 进行对称加密算法签名）	
data 说明						
1	二维码字符串	tdcode	string	Y		
2	场景编号	sceneCode	string	Y	发码平台约定的特定应用场景的编号	
3	订单编号	orderCode	string	Y		
4	订单金额	orderAmount	string	Y		

表 26　提交支付订单输出参数

序号	参数名称	参数	类型	说明	示例值
1	返回码	code	string	01 代表成功	01
2	返回消息	message	string	code = 01，message=”成功”， code = 其他，message=具体错误消息	
3	返回数据	data	string		
data 数据结构定义					

8.9　支付订单回调

用于发码平台向业务系统反馈支付结果。详见表27、表28、表29。

表 27　支付订单回调接口说明

接口调用地址	orderCallback
接口提供者	业务系统
接口消费者	发码平台
功能描述	发码平台将支付结果回调给业务系统

表 28　支付订单回调请求参数

序号	参数名称	参数	参数类型	必填	说明	示例值
1	业务参数	data	string	Y	JSON 格式的业务数据	
2	应用签名	appSign	string	Y	签名值（由平台提供给应用的 AppSecret 用 SM4 进行对称加密算法签名）	
data 说明						
1	订单编号	orderCode	string	Y		
2	支付结果	result	string	Y		
3	失败原因	failReason	string	Y		

表 29　支付订单回调输出参数

序号	参数名称	参数	类型	说明	示例值
1	返回码	code	string	01 代表成功	01
2	返回消息	message	string	code = 01，message=”成功”， code = 其他，message=具体错误消息	
3	返回数据	data	string		
data 数据结构定义					

9　行业码兼容性要求

由于行业特殊性，现阶段存在社保码、交通码、支付码等行业码以及各单位电子证照二维码。各行业、单位二维码规范标准不同，为保障使用便捷性，移动应用程序（APP）支持用户自行申领、展示行业码及电子证照二维码，并与北京民生卡二维码共同使用，保持行业码原有的业务处理流程、应用场景及使用范围不变。

10　移动应用程序要求

10.1　存储

应保障用户公私钥、机构授权数据等信息安全，可采用敏感数据分段存储，且移动应用程序（APP）应保证分段数据组合过程的编程逻辑的安全性。

10.2　显示

移动应用程序显示二维码应满足如下要求：

a) 应支持根据屏幕大小自动将显示的二维码调整至最优显示大小，并保持屏幕高亮、常亮；
b) 二维码图像不得旋转、倾斜、偏转；
c) 二维码内每个模块横向竖向边长应至少各占用 3 个像素点，二维码边长应不小于 3CM。

10.3 时钟

对接统一标准时钟源，保证移动终端的时间和标准北京时间同步。

11 受理终端要求

11.1 通用要求

受理终端应满足如下要求:

a) 应保证在二维码数据的准确识读，并具有一定的自动纠错能力；
b) 二维码读取器区域应与非接触刷卡区域分开，避免应用时互相干扰；
c) 应具备唯一的标识编码，能够通过标识编码追溯到参与交易的受理终端设备；
d) 应根据数字签名、白名单等机制验证二维码来源合法性，确保二维码中不含有木马、病毒和非法链接等有害信息，并应对非法二维码予以明确提示后拒绝交易；
e) 受理终端图片分辨率应大于 200DPI。

11.2 存储

受理终端存储应满足如下要求：

a) 存储容量应不少于 256MByte，循环存储交易记录应不少于 30000 条；
b) 应确保受理终端应用程序、发码机构证书、交易数据、黑/白名单等其他参数的安全存储，不因断电等原因致使数据丢失；
c) 终端不应保存用户敏感信息，对交易敏感数据进行加密存储，确保数据存储安全不被窃取。

11.3 通信

受理终端在通信时应满足如下要求：

a) 具备无线通信模块提供可靠的通讯基础方式，要求网络带宽不应小于 1024 kbps；
b) 终端具备实时将用户扫码行为同步到服务器端；
c) 受理终端应提供应用程序、机构密钥和参数等的下载、更新和删除功能，支持本地或远程下载方式。应对下载进行安全控制，下载应经过授权或认可，未经授权不应更改受理终端中的内容。应能够验证下载程序的完整性和正确性，确保敏感数据在下载过程中不泄漏；
d) 当网络通信模块故障时，受理终端应支持其他数据上传模式。

11.4 时钟

受理终端应满足如下要求：

a) 应具备高精度时钟模块进行精确授时；
b) 应保证正常使用时两次授时误差不大于 2s。

11.5 算法

应符合GB/T 32918、GB/T 32905、GB/T 32907中对SM2、SM3、SM4的规定。

11.6 识读能力

a) 应支持识别二进制编码格式的二维码，支持识别旋转、倾斜、偏转的二维码；
b) 数据解析过程应对二维码中数据信息的完整性、真实性、不可抵赖性和有效性进行鉴别，对于未通过鉴别等非法二维码应予以阻止；
c) 应支持 QR Code 等常用码制；
d) 二维码读取器和受理终端系统应能抵御重放攻击，防止加密数据和交易报文被重用；
e) 应具备识别按照本文件中标准码及简码数据结构生成的二维码能力。

11.7 纠错能力

纠错能力应大于等于7%。

11.8 识读距离

二维码读取器应能够正确识别距离读取器1cm～10cm之间展示的二维码。

11.9 电源要求

应具备断电延时关机功能，保证数据不丢失。

11.10 监控与管理

应具备远程管理能力，包含远程监测终端心跳、终端远程进行软件升级、机构证书下载与更新、黑白名单下载与更新、远程识别终端问题等，并且具有应急处理能力。

12 安全要求

12.1 移动应用安全

移动应用程序应满足如下要求：

a) 应对移动应用程序（APP）进行签名，标识移动应用程序（APP）的来源和发布者，保证客户所下载的移动应用程序（APP）来源于所信任的机构；
b) 移动应用程序（APP）启动和更新时，宜进行真实性和完整性校验，防范移动应用程序（APP）被篡改；
c) 应从木马病毒防范、信息加密保护、运行环境可信等方面提升安全防控能力，并可通过移动应用程序（APP）推送和消息触达等方式提示用户；
d) 应提供软件运行环境安全状况、程序异常等检测功能，并向后台系统反馈移动应用程序（APP）软件状况。

12.2 用户安全

移动应用程序（APP）应验证用户身份。验证可采用如下方式：

a) 用户提供验证信息，例如：移动应用程序（APP）密码或口令等；
b) 用户提供所持设备的验证信息，例如：动态验证码、令牌等；
c) 对恶意用户建立黑名单机制；
d) 应检测用户登录客户端设备，用户更换登陆的客户端设备时，应对用户身份进行确认。

12.3 证书安全

证书应满足如下要求：

a) 由发证机构通过私钥签名，保证证书的合法性和可验证性；
b) 只包含证书拥有者公钥和非敏感信息和发证机构签名；
c) 只包含业务必要的少量属性，从而保证证书只占用很少的用户空间，同时证书在传输过程中也会更小的代码，保证证书在网络中的快速传输；
d) 终端用户要经过实名认证才可以获得数字证书；
e) 应依据 GB/T 32918 标准对证书进行签名；
f) 应保证对证书进行加解密和签名的私钥的安全。

12.4 二维码安全

二维码数据应满如下要求：

a) 含有账户信息的二维码应防重放；
b) 应确保账户信息不被泄露；
c) 数据解析过程应对二维码中数据信息的完整性、真实性、不可抵赖性及时效性进行鉴别，对于未通过鉴别等非法二维码应予以阻止；
d) 应保证二维码在各行业使用时的安全性、独立性。

12.5 支付安全

支付安全应满足如下要求：

a) 参与支付的终端应满足风险控制相应指标；
b) 交易过程中，应提供安全提示机制，确保交易过程中关键环节（如：交易金额及交易类型确认，密码输入等）及交易结果能安全、有效向用户提示，用户确认后才可进行下一步操作。

12.6 通信安全

网络通信协议应满足如下要求：

a) 移动应用程序（APP）与北京民生卡二维码系统服务器间应建立安全的信息传输通道；
b) 通过公开网络进行数据传输时，应通过安全协议传输，如 SSL/TLS 等；
c) 通过移动应用程序（APP）发送的报文关键要素宜进行数字签名，确保关键要素的真实性和抗抵赖性。

12.7 安全管理

应满足如下要求：

a) 应具备实名认证和支付认证的机制；
b) 应具备完整的开发过程包括：开发环境、编码漏洞、安全补丁、质量检测、发布管理等的管理；
c) 应具备软件文档管理，包括用户类文档、工程类文档、管理类文档等的管理。

附 录 A
（资料性）
典型业务应用场景

A.1 社会保障

通过展示北京民生卡二维码，市民可以实现办理养老保险事务、办理求职登记和失业登记手续、申领失业保险、申请参加结业培训、申请劳动能力鉴定和申领享受工伤保险待遇等。

A.2 交通出行

用户乘坐公共交通工具出行时，使用移动应用程序（APP）展示北京民生卡二维码可实现公交、地铁刷码乘车，终端设备扫描北京民生卡二维码后进行业务处理，用户实现乘车及费用支付。

A.3 医疗健康

在医院看病就医应用场景中，与医院HIS系统对接，使用移动应用程序（APP）展示北京民生卡二维码，替代身份证、医院诊疗卡享受入院登记，挂号、就诊、费用结算等医疗服务。

A.4 养老助残

本市及符合条件的60岁以上老人，使用移动应用程序（APP）展示北京民生卡二维码，享受公园景点、公共交通等各类优待政策，本市户籍老年人可凭北京民生卡二维码确认身份权益，享受老年人福利津贴补贴。

A.5 残疾人保障

残疾人使用移动应用程序（APP）展示北京民生卡二维码，作为享受福利待遇的凭证，享受免费交通出行、景区游览、领取残疾人补贴及助残券等残疾人服务项目。

A.6 公共缴费

在停车缴费、小额支付等应用场景中，用户可持移动应用程序（APP）展示北京民生卡二维码，受理终端识别二维码后进行业务处理，实现用户的停车缴费、小额支付应用等。

A.7 公园景点

在进入公园年票所涵盖的景区中，用户可持移动应用程序（APP）展示北京民生卡二维码进行年票确认，实现进园功能。

A.8 校园应用

在校园等封闭式应用场景中，学生可持移动应用程序（APP）展示北京民生卡二维码，实现门禁访客应用、考勤应用、食堂就餐应用、水控电控应用等。

附 录 B
（资料性）
业务应用场景标识示例

表30给出了北京民生卡二维码适用业务应用场景标识的示例，在实际应用中可根据实际场景做对应场景修改及场景扩充。

表 30 业务场景标识示例

标识序列	字段值	状态	对应场景
1	1	已开通	社会保障
	0	未开通	
2	1	已开通	交通出行
	0	未开通	
3	1	已开通	医疗健康
	0	未开通	
4	1	已开通	养老助残
	0	未开通	
5	1	已开通	残疾人保障
	0	未开通	
6	1	已开通	公共缴费
	0	未开通	
7	1	已开通	公园景点
	0	未开通	
8	1	已开通	校园应用
	0	未开通	
9-32			预留

参 考 文 献

[1]JR/T 0149—2016 中国金融移动支付 支付标记化技术规范