国家卫生健康委统计信息中心

国卫统信便函〔2022〕17号

关于印发《电子健康卡建设与管理指南（V3.1）》的通知

各有关单位:

为进一步加强电子健康卡基础设施平台规范化建设和安全运行管理，落实跨地域“一码通行”、多码协同、移动应用安全接入以及信息安全与隐私保护等相关工作要求，我中心组织修订了《电子健康卡建设与管理指南（V3.1）》。现印发你们，供遵照使用。

国家卫生健康委统计信息中心

2022年4月1日

电子健康卡建设与管理指南

（3.1 版）

国家卫生健康委统计信息中心

2022 年 3 月

前言

电子健康卡是国家卫生健康委面向城乡居民设计发放、统一标准的居民就医和健康服务介质，基于跨域主索引体系可对居民进行个人健康身份的唯一标识，旨在为居民建立个人健康的统一身份和服务凭证，是“互联网+医疗”便民服务与全生命周期健康管理的统一服务入口，是“互联网+”新形势下居民健康卡的线上应用延伸与服务形态创新。电子健康卡系统平台是各类医疗卫生机构信息互认共享的重要基础平台，是保障城乡居民实施自我健康管理的重要基础工具，是我国全民健康保障工程的重要基础设施。

为指导各地规范开展电子健康卡应用建设，确保“标准统一、一码通用”，2017 年，国家卫生健康委统计信息中心组织来自于国家密码管理局、中国支付清算协会、中国银联、国家计算机质量检验检测中心、中国软件评测中心、银行卡检测中心以及相关省市卫生健康委信息中心、医疗卫生机构等相关领域专家，共同研究编制了《电子健康卡建设与管理指南》，并在此基础上制定了《电子健康卡技术规范》卫生行业标准。

各省卫生健康委信息中心应根据指南要求结合实际情况组织编制本省电子健康卡项目建设实施方案，报国家卫生健康委统计信息中心论证及备案管理。地市级或医疗卫生机构电子健康卡建设项目可报省卫生健康委信息中心组织项目方案论证并报国家卫生健康委统计信息中心备案管理。各项目建设单位应严格遵循本指南及《电子健康卡技术规范》中各项技术与管理要求开展电子健康卡系统平台建设与运行维护管理。

《电子健康卡建设与管理指南（3.1 版）》包括三个部分材料及 1 个单行本：

材料一《电子健康卡技术指引（3.1 版）》：提出了电子健康卡系统架构，对电子健康卡管理系统和相关的终端、移动应用软件的工作流程、功能、安全提出了技术要求，给出了电子健康卡管理系统的部署建议和接口要求，指导电子健康卡应用过程中各系统、终端、移动应用软件等的开发、部署和网络联通。

材料二《电子健康卡质量控制与安全运行管理要求（2.2 版）》：提出了电子健康卡建设、运行的基本流程和步骤，以及各环节中质量控制和安全运行管理的要求。

材料三《电子健康卡跨域主索引及跨域认证技术要求（2.0 版）》：提出了电子健康卡跨域主索引及跨域认证系统的主要用途、实现方案以及相关技术要求。

《电子健康卡密码模块接口及卡管系统接入认证技术要求 V1.0》内容另见单行本。

本版本指南由国家卫生健康委统计信息中心负责解释，自发布之日起实施。

修订记录

材料一：电子健康卡技术指引

序号	版本	章节	修订内容
1.	1.3	4.2 居民健康卡注册管理系统	增加了电子健康卡应与实体卡具有明确标识区分的要求。
2.	1.3	4.4 电子健康卡管理系统	增加了由虚拟化应用管理系统生成主索引 ID 的要求。 增加了虚拟化应用管理系统与注册管理系统连接的要求。
3.	1.3	6.1.3 密码服务	进一步明确了电子健康卡 ID 的生成规则。
4.	1.4	3 术语	统一术语“电子居民健康卡”为“电子健康卡”。
5.	1.4	5.1 电子健康卡注册流程	明确虚拟化应用管理系统生成主索引 ID，删除了主索引系统，避免产生歧义。
6.	1.4	附录 A	主索引 ID 在虚拟化应用管理系统中生成，删除了主索引系统同时部署的参考方案。
7.	1.5	6.1.3 密码服务	明确了应用密码机是虚拟化应用管理系统的一部分，必须物理环境上同时部署。
8.	1.5	6.1.3 密码服务	明确了有效时间的生成和加密格式。
9.	1.6	6.1.3 密码服务	明确了虚拟化应用管理系统应采用统一的加密机接口调用方式。
10.	1.7	所有章节	统一替换“居民健康卡虚拟化”为“电子健康卡”。
11.	2.0		更名为“电子健康卡技术指引”。
12.	2.0	6.2.1APP 接入管理	增加了电子健康卡 SDK 授权管理的方案要求。
13.	2.0	8.3 电子健康卡管理系统安全要求	明确了电子健康卡系统时间同步的要求。 增加了电子健康卡 API 安全认证的方案要求。
14.	2.0	附录 C	对 8.3 中时间同步进行介绍，提出了一种可行方案。
15.	2.1	3.6	明确了电子健康卡 APP 的多种形态。
16.	2.1	3.8	新增了“电子健康卡 API”。
17.	2.1	3.11，4.8，5.2，5.3，6.1.2	增加“多码合一”的相关内容。
18.	2.1	5.3	明确了静态码在使用过程中必须进行补充身份鉴别的要求。
19.	2.1	8.4 电子健康卡密码机部署安全要求	将《电子健康卡密码机技术规范》中第 6 章节密码机部署要求迁移至本指引。 进一步明确了单密码机部署和多密码机部署要求。
20.	2.1	附录 D	将《电子健康卡密码机技术规范》中第 5 章节编程接口要求迁移至本指引。

序号	版本	章节	修订内容
21.	2.2	附录 E	将《电子健康卡 API 授权管理系统技术指引》中的主要内容迁移至本指引。
22.	2.2	E7.1	修复了 Apply_type 没有标注必选项的问题。并给出了该项的字典。
23.	2.2	图 4.1	删除了重复的 4.1 图。4.1 图医保中心与电子健康卡增加了连接线。
24.	2.2	6.1.2.1	增加了三码合一中支付数据的域。
25.	2.2	6.2.1	删除重复的文字。
26.	2.2	8.4	删除重复的文字。
27.	2.2	图 8.1	统一电子健康卡管理信息系统的名称。
28.	2.2	E7.4.3	修复错误的 ehealth_code 长度。
29.	2.3	2 规范性引用标准	加入了网络安全法、等级保护基本要求、信息系统密码应用基本要求、条码支付安全技术规范、条码支付受理终端技术规范等文件。
30.	2.3	图 4.1	加入了商保机构。 “密码服务”调整为“二维码密码服务”。 接入层增加了“接入认证服务”。
31.	2.3	6.2 接入层要求	将 API 授权管理作为接入层总体要求提出，提炼了 API 授权管理的的核心要素。
32.	2.3	6.2.4 接入认证服务	新增了接入认证服务的要求。
33.	2.3	8.1 通用要求	加入了 GM/T 0054-2018 第三级安全要求。
34.	2.3	附录 B	增加和完善了附录内容，详细描述了卡面和二维码的设计规范。
35.	2.3	附录 E（资料性附录）电子健康卡 API 授权管理方案	修改了电子健康卡 API 授权管理的部分描述，使授权管理是电子健康卡管理信息系统的组成部分更加明确。
36.	2.4	4.1 居民健康卡跨域主索引系统	对生成主索引的证件部分加入了“港澳居民居住证、台湾居民居住证、出生医学证明”。
37.	2.4	4.7 金融交易机构	进一步修订了描述，强调金融交易机构作为服务提供方提供支付功能。
38.	2.4	4.8 保险机构	修订医保中心为保险机构，泛指提供保险服务的机构。
39.	2.4	全部	删除“多码合一”的实现方式，多码合一将另行制定规范。
40.	2.4	5 电子健康卡数据标准及工作流程	原“5 电子健康卡数据工作流程”改为“5 电子健康卡数据标准及工作流程”。
41.	2.4	5.1 电子健康卡数据标准	将“6.1.2.1 二维码数据内容要求”移至本章节，突出其总体地位。 删除了“多码合一”中的支付和保险字段。 对扩展字段重新进行描述。扩展字段中增加默认扩展字段“签发渠道”，用于标识电子健康卡验证路径，并用于跨卡管的路由。

序号	版本	章节	修订内容
42.	2.4	5.2.3　电子健康卡二维码使用流程	增加了关于跨卡管系统进行电子健康卡验证的流程说明。
43.	2.4	6.1.1 电子健康卡账户管理	登记信息增加了属性标签（如健康扶贫对象），在二维码验证时，可以返回此属性标签给医疗机构。
44.	2.4	6.1.2.1 二维码生成	原“6.1.2.2 二维码生成”章节，内容无变化。
45.	2.4	6.1.2.2 二维码验证	原“6.1.2.3 二维码验证”章节。 增加了描述，验证结果是向医疗机构返回个人信息。 增加了关于跨卡管系统进行电子健康卡验证的流程说明。
46.	2.4	6.2 接入层要求	重述了本部分内容，明确“白名单”是接入电子健康卡管理信息系统的基本控制方式，推荐采用基于密码的技术方式实现接入控制。
47.	2.4	6.2.1 客户端应用软件接入管理	明确了客户端应用软件接入管理模块信息登记的要求。
48.	2.4	6.2.2 机构接入管理	明确了机构接入管理模块信息登记的要求。
49.	2.4	6.2.3 识读终端管理	明确了识读终端管理模块信息登记的要求。
50.	2.4	9.1 数据同步要求	原 4.4 中数据同步要求移至 9.1 章节。 增加了参照附录 F （规范性附录）电子健康卡数据同步接口规范进行数据同步的说明。
51.	2.4	附录 B　（规范性附录）电子健康卡展示界面及卡面规范	进一步细化了电子健康卡界面展示的要求。
52.	2.4	附录 C　（资料性附录）电子健康卡时钟同步系统部署方案	重新绘制了部署架构图。
53.	2.4	附录 D　（规范性附录）电子健康卡密码机高级应用编程接口	强调了实现方式中数据补位问题。
54.	2.4	附录 E　（资料性附录）电子健康卡管理信息系统接入层认证方案	对基本的认证实现思路进行了概括性描述，使其更具有通用性，可以应用于 APP、机构、终端等不同的接入控制模式。
55.	2.4	附录 F （规范性附录）电子健康卡数据同步接口规范	增加了各级卡管与国家卡管进行数据同步的接口。

序号	版本	章节	修订内容
56.	2.4	附录 G （规范性附录）电子健康卡跨域验证接口规范	增加了通过国家卡管进行跨域查询的接口。
57.	2.4.0.1	5.2.3 电子健康卡二维码使用流程	图 5.3 用户使用电子健康卡二维码中的补充身份鉴别部分，静态二维码改为“推荐”，更符合实际使用需求。
58.	2.5	3 规范性引用文件	删除了没有引用的实体卡密钥相关规范。
59.	2.5	图 4.1 电子健康卡系统平台架构图	调整图片中“居民”部分电子健康卡展示样式与附录 B 一致。
60.	2.5	6.1.2 二维码管理	对“有效时间”增加补充说明，“二维码超过有效时间后不可用”。
61.	2.5	6.1.3 二维码密码服务	对示例“如当前时间为 2018 年 1 月 17 日 11:50:03，则表示为 20180117115003（HEX）”中“当前时间”改为“有效时间”，避免引起误解。
62.	2.5	附录 H （规范性附录）信息系统编码规则	将 2.4.0.1 版本中材料二与信息系统编码相关内容转移到本附录。本附录中描述的信息系统编码规则作为标准实施的一部分。 本附录为规范性附录，各机构必须按照此附录实现相关的系统编码规则。
63.	3.0	全部	调整所有“密码机”为“密码模块”，提供更多中形态的密码产品为电子健康卡系统提供密码服务，即包含密码机、密码卡等。
64.	3.0	6.1.3.2 密码模块管理	新增本节内容，明确了电子健康卡管理信息系统中密码服务模块应具有的密码模块管理登记功能。
65.	3.0	D.2 密码卡高级应用编程接口	增加密码卡作为密码模块调用时的接口。
66.	3.0	附录 H.2 电子健康卡管理信息系统接入组件编码规则	增加密码模块的登记编号规则，配合 6.1.3.2 章节对密码模块的登记使用。采用 CRP 作为密码模块（Crypto Module）的缩写。
67.	3.0.1	2.规范性引用文件	修改网络安全等级保护规范编号及名称； 增加 JR/T 0171-2020 个人金融信息保护技术规范； 删除 PCAC/T 0001-2016 个人信息保护技术指引
68.	3.0.1	4.1,4.2	原内容转入章节 4.1； 新增 4.2，覆盖原附录 G 的相关内容；对电子健康卡跨域认证图进行了修改。
69.	3.0.1	6.2 接入层要求	修改表 6.2 客户端应用软件登记信息要求，增加‘可空’列； 修改表 6.3 删除机构编码，机构接入系统地址；增加所属省份行政区划代码、所属城市行政区划代码、机构组织机构代码。
70.	3.0.1	6.3 数据接口要求	删除 10.1 数据同步要求，新增至 6.3 数据接口

序号	版本	章节	修订内容
			要求； 数据接口以《电子健康卡网络接口标准》单行本方式发布。
71.	3.0.1	附录 F 电子健康卡网络编码规则	删除原附录 F （规范性附录）电子健康卡数据同步接口规范内容、原附录 G （规范性附录）电子健康卡跨域验证接口规范内容，附录内容以单行本方式发布； 原附录 H 信息系统编码规则内容调至附录 F； 附录 F 名称变更为电子健康卡网络编码；明确各管理节点网络编码由国家委负责分配，各服务节点编码由各级卡管负责分配。增加了主管机构的类型包括 A 卫健委；B 医院；C 公共卫生机构；D 基层卫生机构；E 政府其他部门；F 第三方机构；X 其他。增加了识读终端的类型 STM。
72.	3.1	2 规范性引用文件	删除居民健康卡技术规范的引用。
73.	3.1	4.1 电子健康卡管理平台架构图	删除“居民健康卡注册管理系统”和“居民健康卡密钥管理系统”； 修改“居民健康卡跨域主索引系统”为“电子健康卡跨域主索引及跨域认证系统”； 修改电子健康卡系统平台架构图。
74.	3.1	4.1.1 电子健康卡跨域主索引及跨域认证系统	修改“居民健康卡跨域主索引系统”为“电子健康卡跨域主索引及跨域认证系统”； 增加了跨域认证相关内容。
75.	3.1	4	删除“居民健康卡注册管理系统”内容； 删除“居民健康卡密钥管理系统”内容。
76.	3.1	4.1.2 电子健康卡管理信息系统	删除居民健康卡注册管理系统相关内容。
77.	3.1	4.2 电子健康卡服务网络架构图	修改图 4.3 电子健康卡跨域认证网络架构图； 修改电子健康卡跨域认证验证环节。
78.	3.1	5.1.2 二维码数据标准	增加了电子健康卡客户端应用软件的编号（EHCAPPID）和电子健康卡管理信息系统的入网编码（EHCIN）附录 D 的引用。
79.	3.1	5.2.1 电子健康卡注册流程	修改电子健康卡注册流程； 修改图 5.1 注册电子健康卡账户流程图。
80.	3.1	5.2.3 电子健康卡二维码使用流程	修改二维码跨域验证流程； 修改图 5.3 用户使用电子健康卡二维码流程图。
81.	3.1	6.1 电子健康卡账户管理	增加了电子健康卡账户管理的账户绑卡功能； 增加了电子健康卡账户信息在电子健康卡跨域主索引及跨域认证系统中注册的要求
82.	3.1	6.2 二维码管理	将二维码管理从 6.1 中移出，单独成为 6.2 小节。
83.	3.1	6.2.3 密码服务	将密码服务部分内容以单行本方式发行。
84.	3.1	6.3 机构接入管理	增加了机构信息批量导入和黑名单功能。
85.	3.1	6.4 识读终端管理	增加了识读终端信息批量导入功能。

序号	版本	章节	修订内容
86.	3.1	6.5 密码模块管理	将密码模块管理从 6.2.3 中移出，单独成为 6.5 小节。
87.	3.1	6.6 数据接口要求	将“电子健康卡管理信息系统应与国家级综合管理系统连接”调整为“电子健康卡管理信息系统应与国家电子健康卡应用监测系统连接”； 将“国家级系统通过接口方式主动查询”调整为“国家电子健康卡应用监测系统通过接口方式主动查询”及附录引用。
88.	3.1	6.7 数据审计	增加了电子健康卡管理信息系统数据审计功能及说明。
89.	3.1	7 客户端应用软件接入与管理要求	客户端应用软件接入和管理要求单独成章，并明确、细化了部分要求。
90.	3.1	7.2 接入管理	增加了对违规的客户端应用软件进行暂停接入和重新启用的要求。
91.	3.1	7.3 安全要求	增加了电子健康卡管理信息系统接入层认证方案的引用。
92.	3.1	8 电子健康卡运行可靠要求	增加了电子健康卡运行可靠要求，明确了电子健康卡运行可靠性及承载能力的要求
93.	3.1	9.1 通用要求	增加了系统采用国密标准的 SSL/TLS 协议的要求。
94.	3.1	9.2 身份认证要求	增加了电子健康卡管理信息系统的身份认证要求及附录引用。
95.	3.1	9.4 电子健康卡管理信息系统安全要求	增加了双因素身份鉴别要求。
96.	3.1	9.5 电子健康卡密码模块部署安全要求	删除了对密码机前置代理服务与密码机安全防护等级相同的要求。 增加了密码模块对卡管系统安全接入认证要求。
97.	3.1	9.6 网络通信安全要求	修改了客户端与服务器之间通过公开网络进行数据传输时应进行双向认证，建议使用数字证书。
98.	3.1	9.7.4 安全要求	更正了二维码生成和验证时，对参与运算密钥的描述，将“用户身份认证密钥”改为“保护密钥”；将应对传输的数据进行保密性保护改为安全性保护，数据传输安全性包括保密性、完整性和不可抵赖性。
99.	3.1	附录 E （规范性）全国电子健康卡应用监测系统数据采集标准规范	删除原附录 D 和附录 E，改为单行本方式发行； 原附录 F 调整到附录 D，附录 G 调整到附录 E； 删除原附录 H。
100	3.1	附录 F （资料性）电子健康卡管理信息系统身份认证方	增加了资料性附录：电子健康卡管理信息系统身份认证方案。

序号	版本	章节	修订内容
		案	

材料二：电子健康卡质量控制与安全运行管理要求

序号	版本	章节	修订内容
1.	1.0	1 建设流程 2 管理要求	新增。
2.	1.0	3 检测要求	原《电子健康卡技术指引》的检测要求内容。
3.	1.1	2 运行阶段	增加运行管理要求。
4.	1.1	3 检测流程	增加检测流程图。
5.	1.2	全部	统一了术语。修订“电子健康卡系统”为“电子健康卡系统平台”,“电子健康卡管理系统”为“电子健康卡管理信息系统”。
6.	1.3	全部	根据《电子健康卡技术指引》调整部分术语描述。
7.	1.3	3 3 电子健康卡系统平台管理要求	新增了电子健康卡系统平台管理要求。
8.	1.4	1 电子健康卡产品标准符合性测试	明确对电子健康卡产品的管理要求为标准符合性管理。
9.	1.4	2 电子健康卡系统平台建设流程	调整和优化了电子健康卡系统平台建设的流程，要求电子健康卡系统平台与国家级平台先联通后检测。
10.	1.4	2.2 电子健康卡系统平台建设	修订建设流程，生产商直接向检测机构提交检测申请及要求的资质证明文件。
11.	1.4	2.6 现场联网检测	增加现场联网检测通过后，对新增已过检的识读终端、密码机、客户端软件的备案要求； 增加子项目定义及要求。
12.	1.4	4 电子健康卡系统平台管理要求	修订管理要求，增加抽检。
13.	1.4	5 电子健康卡技术检测要求	增加检测报告有效期； 增加检测机构应向申请机构出具检测报告及上传电子健康卡标准符合性检测管理平台。
14.	1.5	1 电子健康卡产品标准符合性测试	进一步明确了标准符合性测试的管理方式。
15.	1.5	2 电子健康卡系统平台建设运行流程	整合了原建设流程和运行流程两个章节。 将对系统平台的标准符合性测试要求融入其中。 明确了客户端应用软件的标准符合性测试要求。 明确了联网评估的思路和方法。 进一步强调了建设单位的管理责任。
16.	1.6	1 电子健康卡产品标准符合性测试	明确了产品著作权的要求。
17.	1.7	1 电子健康卡产品标准符合性测试	增加了检测流程图。
18.	1.7	2 电子健康卡系	增加了建设流程图。

序号	版本	章节	修订内容
		统平台建设流程	
19.	1.7	3　电子健康卡移动应用运行监测	原“2.9 客户端应用软件运行监测”内容。 完善了电子健康卡应用软件的运行监测流程。
20.	1.7	附录A 电子健康卡移动应用监测告知书	根据电子健康卡移动应用运行监测流程的调整，删除此附录。
21.	1.7	附录	增加了电子健康卡联网检测的承诺书和评估模板。
22.	1.8	1.2 备案管理	增加了电子健康卡产品备案管理的要求，明确了不同产品的备案编码规则。
23.	1.8	2　电子健康卡系统平台建设流程	重新绘制了建设流程图，更加清晰地描述建设阶段的主要工作。
24.	1.8	2.1 项目实施方案论证	增加了项目备案号的要求，明确了项目备案编码规则。
25.	1.8	2.3 客户端应用软件接入	对客户端应用软件接入部分的要求进行了重述。 明确了建设单位对客户端应用软件安全的责任。 明确了客户端软件重大版本变更时报备的要求。 明确了客户端软件在电子健康卡管理信息系统中的登记备案要求。
26.	1.8	2.5 系统平台联通	明确了各建设单位应向国家平台报送的信息内容。
27.	1.8	3　电子健康卡移动应用运行监测	对电子健康卡移动应用运行监测的部分进行了重述。
28.	1.8.0.1	1.2.1　电子健康卡管理信息系统编码	编码长度应为6位，但表格中为7位。表格有误，进行了调整，删掉了多余的级别编码。
29.	1.8.0.1	2.3.2　客户端应用软件授权接入管理	明确了服务号保存EHCAPPID和设计多个EHCAPPID时的要求。
30.	1.9	1 电子健康卡标准符合性测试	修改为“1　电子健康卡质量管理基本要求”，删去了对开发商备案的描述，增加了关于建设单位的责任要求，增加了标准符合性证明材料的要求。
31.	1.9	2　电子健康卡系统平台建设流程要求	总体建设流程图删除了“移动应用监测平台”。
32.	1.9	2.1.2　方案论证与备案	整合了原有的2.1.2方案论证与2.1.3项目备案两部分内容。
33.	1.9	2.2 系统平台建设	“改造电子健康卡的受理应用环境，实现电子健康卡在医疗机构的场景落地”中“医疗机构”改为“业务应用机构”，进一步扩展电子健康卡的实际应用范围。
34.	1.9	2.3 客户端应用软件接入	将“备案”改为“登记”，参照“材料一”附录H进行登记工作。增加对接入客户端证明材料的要

序号	版本	章节	修订内容
			求。
35.	1.9	2.6 联网评估	正文中增加了对“附录：电子健康卡联网评估承诺函”的引用。
36.	1.9	3 电子健康卡运行管理要求	增加了“3.1 电子健康卡系统平台运行管理要求”；修订了“3.2 运行安全风险控制”的描述。
37.	2.0	2.7 密钥灌装及密码模块管理	增加了对密码模块管理的要求。密码模块信息应进行登记，并在发生变更时按照安全的方式进行处理，防止密钥的丢失。
38.	2.1	1.2 电子健康卡网络安全责任	架构图内容在《电子健康卡技术指引》4.2 中进行了描述，本部分删除。
39.	2.2	1.1 产品标准符合性要求	增加了对建设单位所使用的电子健康卡系统平台进行抽查的要求。
40.	2.2	2.1 项目备案申请	增加了项目备案申请的说明。
41.	2.2	2.2.2 方案论证与备案	增加了上传材料到国家居民健康综合管理平台的说明。
42.	2.2	2.6 系统平台联通	将“电子健康卡用卡监测数据”调整为“国家电子健康卡应用监测系统”。
43.	2.2	2.7 联网评估	补充承诺函参考模板的附录引用； 将上传“承诺函”和“自评估报告”的步骤整合在 2.8 章节。
44.	2.2	2.8 密钥灌装及密码模块管理	增加了密钥灌装申请时上传材料到国家居民健康卡综合管理平台的说明及目录引用。
45.	2.2	3.1 电子健康卡系统平台运行管理要求	增加了建设单位应确保电子健康卡管理信息系统符合网络安全等级保护测评三级要求和符合商用密码应用安全性评估要求。
46.	2.2	附录 A	增加了附录 A 电子健康卡联网检测现场自评估报告和承诺函模板。
47.	2.2	附录 B	增加了附录 B 电子健康卡管理信息系统自评估报告和承诺函模板。
48.	2.2	附录 C	增加了附录 C 电子健康卡客户端应用软件（APP）接入自评估报告和承诺函模板。
49.	2.2	附录 D	增加了附录 D 电子健康卡客户端应用软件（第三方服务号）接入自评估报告和承诺函模板。
50.	2.2	附录 E	增加了附录 E 固定式条码扫描设备自评估报告模板。
51.	2.2	附录 F	增加了附录 F 密码模块自评估报告模板。

材料三：电子健康卡跨域主索引系统及跨域认证管理服务技术指引

序号	版本	章节	修订内容
1.	1.3	附件 D 索引号生成方案	调整生成因子内容的顺序与电子健康卡顺序一致。
2.	1.4		将“主索引平台”调整为“主索引系统”。

3.	1.5	4.1.4	“人索引”中删除了婚姻状态、职业、住址等变化性因素。
4.	2.0		将材料三改名为“电子健康卡跨域主索引及跨域认证技术要求”。
5.	2.0	1	重新梳理目录结构及内容，第一章节改为电子健康卡跨域主索引。
6.	2.0	2	增加电子健康卡跨域认证服务。
7.	2.0	3	增加密码服务内容。
8.	2.0	附录 A	增加电子健康卡跨域认证接口规范。

《电子健康卡建设与管理指南》材料一

电子健康卡技术指引

（3.1 版）

国家卫生健康委统计信息中心

2022 年 3 月

目录

电子健康卡技术指引

1 范围

本指引包括电子健康卡技术架构、工作流程、技术功能要求、应用安全要求、电子健康卡系统平台管理要求等。

本指引用于规范建设单位开展电子健康卡应用相关业务时，所需软硬件的设计、研发、集成和维护。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡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。

中华人民共和国主席令第53号 中华人民共和国网络安全法

中华人民共和国主席令第29号 中华人民共和国电子签名法

中华人民共和国主席令第35号 中国人民共和国密码法

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求

3 术语和定义

电子健康卡

通过用户身份标识建立的居民健康卡电子账户。健康卡电子账户使用时，可通过二维码形式展现为电子健康卡。

主索引 ID

主索引ID是标识居民健康用户唯一性的信息，通过主索引ID关联用户的实体居民健康卡、电子健康卡、医院就诊卡等不同类型账户。

电子健康卡 ID

电子健康卡系统平台中用于标识电子健康卡账户唯一性的信息。电子健康卡ID由用户的证件类型和证件号码的密文组成。

电子健康卡二维码

电子健康卡通过二维码的形式予以展示，通过“面对面”方式进行交互使用。电子健康卡二维码包括静态二维码和动态二维码：静态二维码可通过客户端应用软件呈现，也可印刷或粘贴于就诊卡等介质上，必须配合密码、短信验证码、生物识别等方式使用；动态二维码由客户端应用软件呈现，在每次使用前生成，其生命周期根据应用安全的要求限定时间范围。

电子健康卡客户端应用软件（APP）

设备中运行的完整的且包含电子健康卡功能的客户端应用软件。设备类型包括手机、自助终端及其他类型的终端。电子健康卡客户端应用软件包括但不限于原生客户端应用软件、第三方服务号等表现形态。

电子健康卡 SDK（Software Development Kit，软件开发工具包）

实现电子健康卡功能的软件开发包，可以在开发过程中进行调用。

电子健康卡 API（Application Programming Interface，应用程序编程接口）

电子健康卡管理信息系统提供的用于客户端应用软件接入的功能接口，客户端应用软件通过电子健康卡SDK进行调用。

识读终端

识读二维码并与后台应用系统进行交互的终端，一般包括二维码的识读设备和终端机上的应用软件。

二码合一

电子健康卡二维码集成支付功能。通过对同一二维码的识读，实现居民健康卡账户认证与支付双重功能。

多码合一

电子健康卡二维码集成支付功能和保险功能。通过对同一二维码的识读，实现居民健康卡账户认证与支付双重功能。

电子健康卡服务网络

由电子健康卡管理信息系统和电子健康卡客户端应用软件（APP）、识读终端、医疗机构等互联互通构建的网络，为居民提供身份认证等基础服务。

4 电子健康卡系统平台架构

4.1 电子健康卡系统平台架构图

电子健康卡利用电子健康卡跨域主索引系统、电子健康卡密码管理系统和电子健康卡管理信息系统，以二维码技术为核心，实现电子健康卡的应用。

电子健康卡系统平台架构如图4.1所示：

图 4.1 电子健康卡系统平台架构图

注：此图仅表述各系统间的关系，不代表实际的部署架构。各区域级电子健康卡管理信息系统部署架构参见附录A。

4.1.1 电子健康卡跨域主索引及跨域认证系统

电子健康卡跨域主索引是实现管辖范围内居民信息统一识别的独立的信息管理系统。基于该系统可实现对所辖各区域居民标识域，以及身份证、社保卡、军官证、港澳居民来往内地通行证、台湾居民来往内地通行证、出生医学证明、就诊卡等标识证的统一注册管理，通过主索引ID进行唯一性标识。

电子健康卡跨域认证是在非发卡地进行电子健康卡二维码识别时，实现跨地域识别。

电子健康卡跨域主索引及跨域认证系统要求详见《材料三：电子健康卡跨域主索引及跨域认证服务技术要求V2.0》。

4.1.2 电子健康卡管理信息系统

电子健康卡管理信息系统是电子健康卡的核心系统，具有电子健康卡账户管理、二维码管理、密码服务、跨域认证服务等功能，并对外部接入的机构、识读终端、客户端应用软件等进行管理。

4.1.3 医疗卫生机构

4.1.4 机构终端

医疗卫生机构部署机构终端用于申请二维码。机构终端可包括自助终端、挂号窗口终端等多种形式，实现电子健康卡在医疗机构场景的发行。

4.1.5 识读终端

医疗卫生机构可通过识读终端识读用户提供的二维码，并将二维码信息传输至电子健康卡管理信息系统，用于识别用户身份。

4.1.6 个人终端

个人终端（包括手机、平板电脑等移动设备）运行的电子健康卡客户端应用软件接入电子健康卡管理信息系统。电子健康卡客户端应用软件可注册电子健康卡账户，申请电子健康卡二维码，并可管理与居民健康卡绑定的各医院就诊卡账户，查询居民在各医院的就诊信息。

4.1.7 金融交易机构

金融交易机构可接入电子健康卡管理信息系统，作为支付服务提供方，向电子健康卡用户提供支付服务，实现电子健康卡功能与金融支付功能的融合，即“二码合一”。金融交易机构也可直接与医疗卫生机构建立支付结算通道。

4.1.8 保险机构

保险机构包括医保机构和商保机构。保险机构作为保险服务提供方，向电子健康卡用户提供保险结算服务，实现电子健康卡功能、金融支付功能、保险结算功能的融合，即“多码合一”。

4.2 电子健康卡服务网络架构图

国家级系统与各区域级系统连接形成电子健康卡服务网络，如图4.2所示。

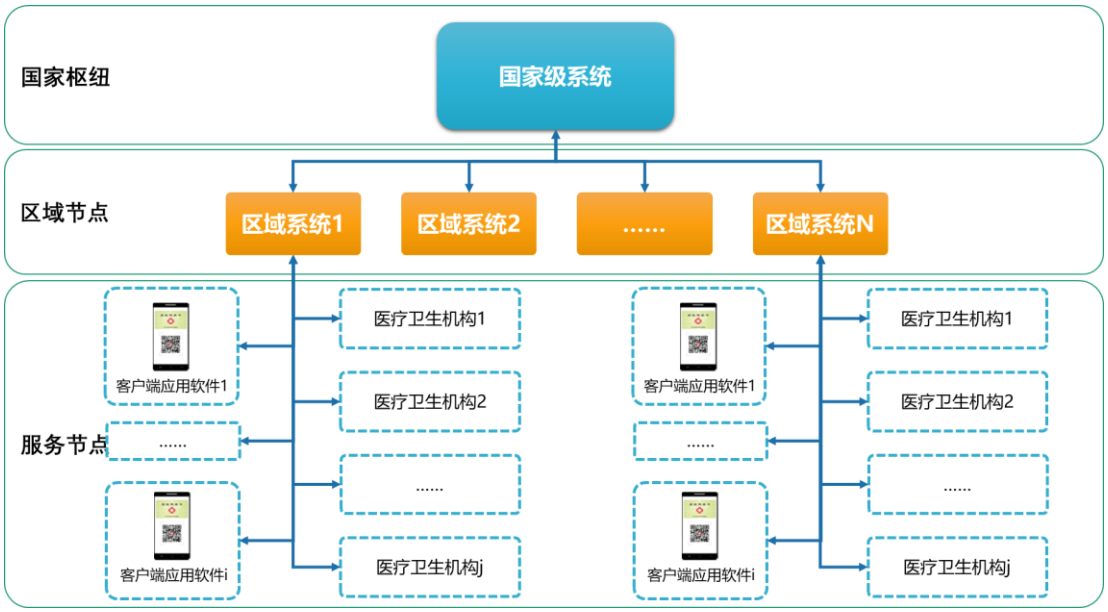


图 4.2 电子健康卡服务网络架构图

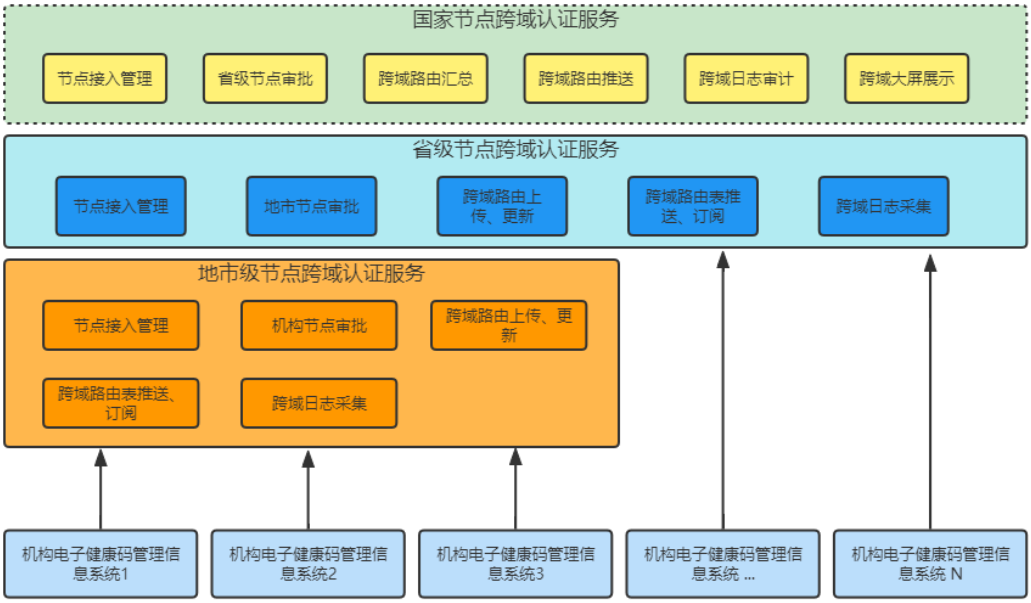


图 4.3 电子健康卡跨域认证网络架构图

用户在发卡机构电子健康卡管理信息系统（以下简称“卡管”）申领电子健康卡后，在用卡机构卡管的用卡场景下扫码验证，依次进行以下验证环节：

第一步，用卡机构卡管对用户展示的电子健康码进行验证，如果用卡机构和发卡机构是同一个卡管，直接返回电子健康码验证结果；否则，用卡机构调用跨域认证服务进行验证；

第二步，用卡机构根据电子健康卡跨域主索引和跨域认证系统路由至发卡机构卡管请求验证；

第三步，发卡机构卡管对二维码进行验证，返回验证结果至用卡机构，完成验证，并在用卡机构为用户建立一张本地电子健康卡。跨域认证网络架构图如图 4.3 所示。

5 电子健康卡数据标准及工作流程

5.1 电子健康卡数据标准

5.1.1 符号说明要求

字段出现要求：“M”表示本字段必须出现，“O”表示本字段根据情况选择是否出现。

字段分隔字符：二维码不同字段使用“英文半角冒号”作为分隔字符。

5.1.2 二维码数据标准

电子健康卡二维码数据的内容格式应符合表 5.1要求。

表 5.1 二维码数据标准

序号	字段内容	代码	出现要求	备注
1	电子健康卡 ID	EHCID	M	本标准中用 EHCID 表示。

2	二维码类型标识符	TAG	M	0 为动态二维码标识符，1 为静态二维码标识符
3	二维码有效性信息	VALID	O	由二维码密码服务模块对有效时间加密产生，动态码必须存在，静态码置为空。
4	扩展字段	EXT	M	扩展字段。默认为签发渠道号。
5	扩展字段 1-签发渠道号	EHCAPPID	M	电子健康卡客户端应用软件视为电子健康卡的签发渠道，签发渠道号即电子健康卡客户端应用软件的编号（EHCAPPID）。EHCAPPID 的前 9 位为电子健康卡管理信息系统的入网编码（EHCIN），EHCIN 用于跨电子健康卡系统平台进行路由，详见附录 D。

示例：

静态二维码　EHCID:1::EHCAPPID

动态二维码　EHCID:0:VALID:EHCAPPID

5.2 电子健康卡工作流程

5.2.1 电子健康卡注册流程

注册电子健康卡的主要流程如图 5.1所示：

1) 用户通过客户端应用软件或机构终端向电子健康卡管理信息系统提交实名制信息进行注册。用户实名制认证可通过线下方式（如通过自助终端读取用户证件）或线上方式（如通过金融交易机构对身份信息和银行账户信息进行验证）完成。
2) 电子健康卡管理信息系统接受请求，在本地卡管系统查询是否存在该用户：
   如存在，电子健康卡管理信息系统返回用户信息和电子健康卡ID。
   如不存在，电子健康卡管理信息系统根据通过实名制验证的用户信息生成主索引ID和电子健康卡ID，完成用户注册。
3) 电子健康卡管理信息系统与电子健康卡跨域主索引及跨域认证系统同步电子健康卡账户信息。

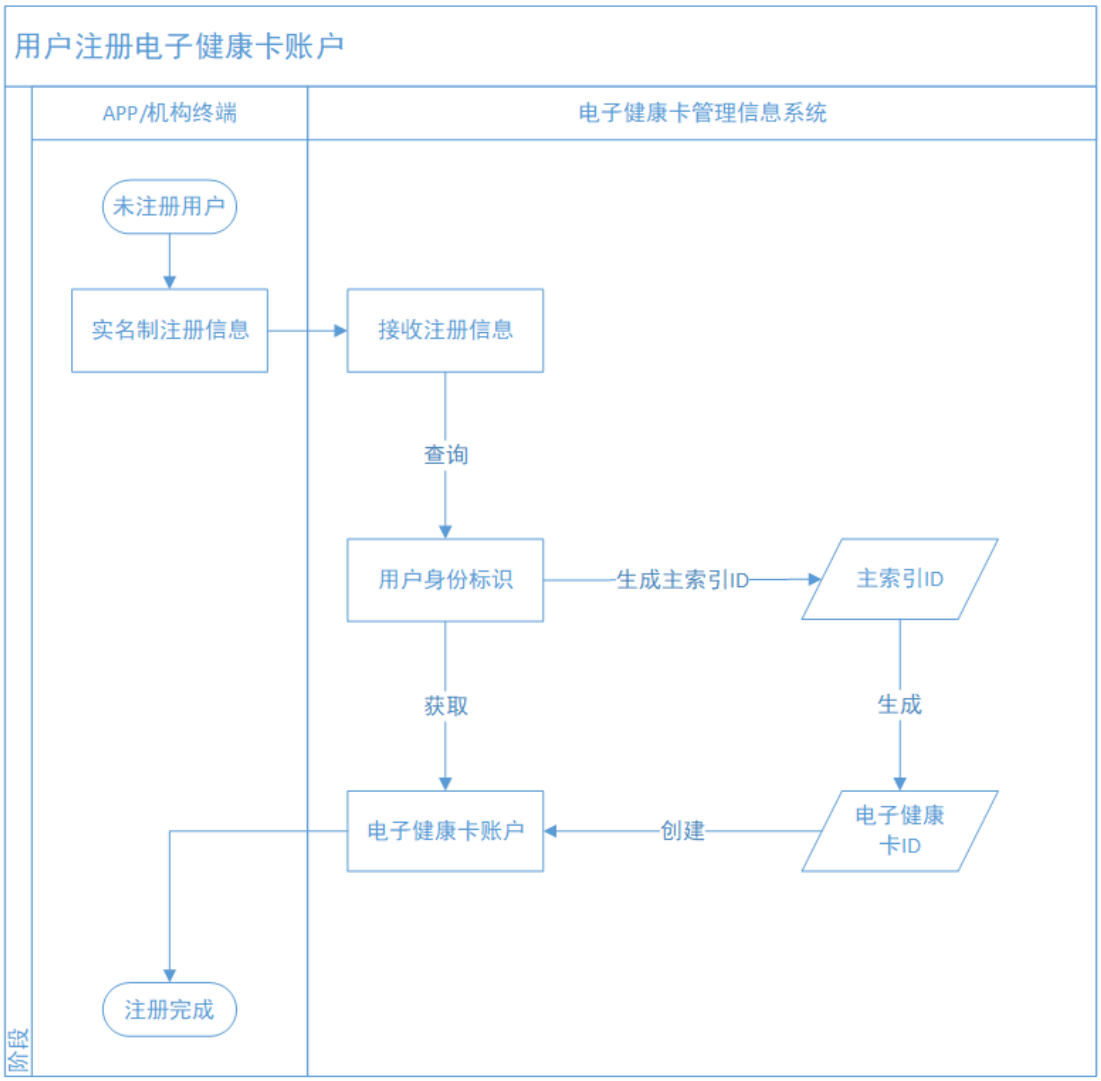


图 5.1 注册电子健康卡账户

5.2.2 电子健康卡二维码申请流程

电子健康卡二维码申请的主要流程如图 5.2所示：

1) 用户通过客户端应用软件或机构终端申请二维码。
2) 电子健康卡管理信息系统（二维码管理模块）根据业务功能确定的二维码类型（静态二维码或动态二维码）进行二维码生成。
3) 电子健康卡管理信息系统将二维码返回客户端应用软件或机构终端。

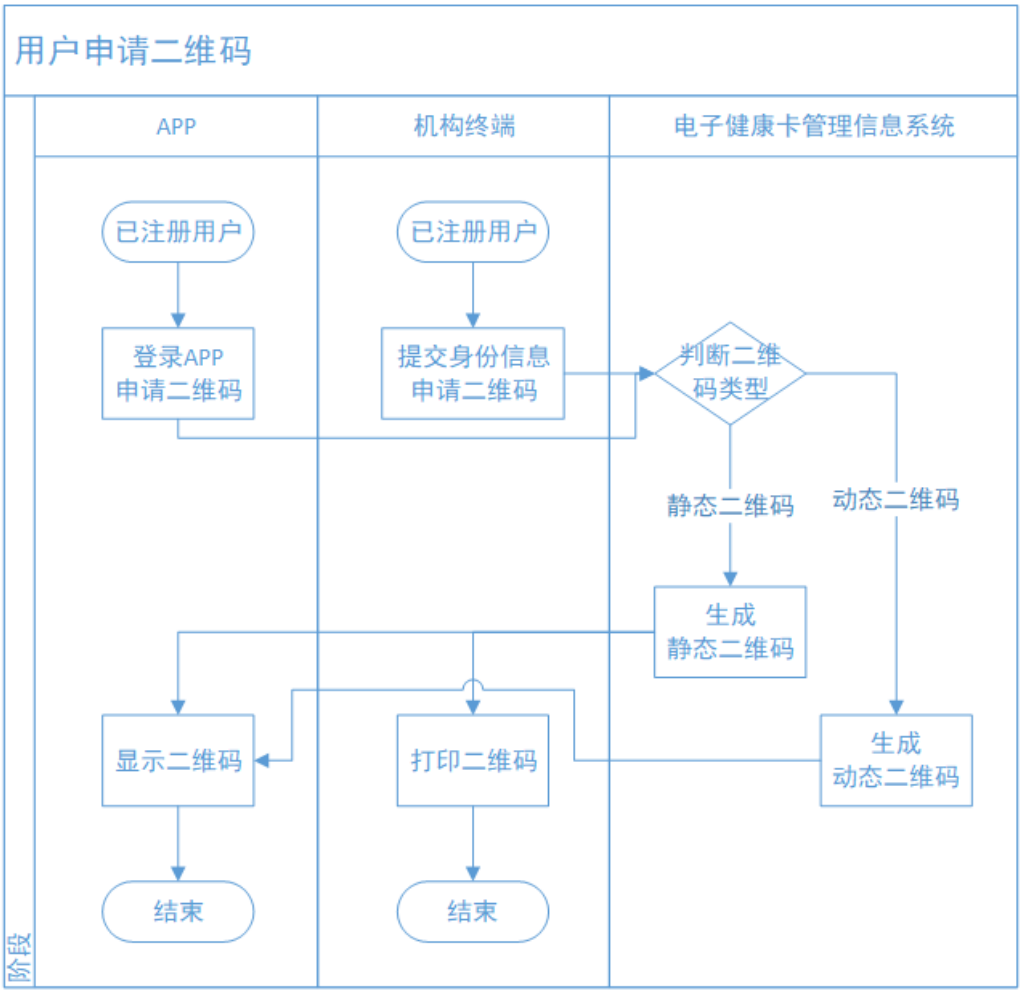


图 5.2 用户申请电子健康卡二维码

5.2.3 电子健康卡二维码使用流程

电子健康卡二维码使用的主要流程如图 5.3所示：

1) 识读终端识读用户出示的二维码。
2) 电子健康卡管理信息系统（二维码管理）根据EHCIN，确定是否为本机构注册的二维码。如果非本机构的二维码，则通过电子健康卡跨域主索引及跨域认证系统进行跨域验证。如果为本机构的二维码，则由本机构直接进行验证。
3) 电子健康卡管理信息系统（二维码管理）根据二维码类型确定是否需要对用户进行补充身份鉴别，静态码推荐补充身份鉴别，动态码可选补充身份鉴别。
4) 电子健康卡管理信息系统（二维码管理）对电子健康卡二维码中的数据进行验证。
5) 电子健康卡管理信息系统（二维码管理）返回验证结果。

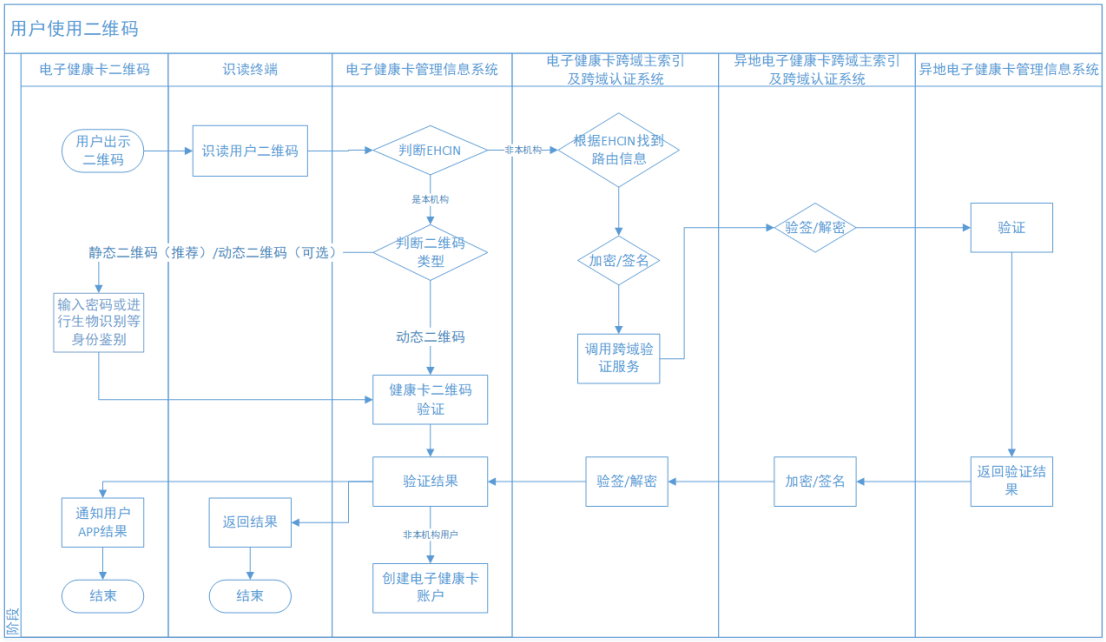


图 5.3 用户使用电子健康卡二维码

6 电子健康卡管理信息系统功能要求

本节描述电子健康卡管理信息系统必备的基本功能。

6.1 电子健康卡账户管理

电子健康卡管理信息系统具有电子健康卡账户的管理功能，即对电子健康卡的账户信息管理和账户生命周期管理。

电子健康卡账户信息包括电子健康卡ID、用户身份信息（姓名，手机号，经验证的证件号码、证件类型等）、主索引ID、用户属性标签（如健康帮扶对象）等。电子健康卡ID由账户管理功能调用密码服务功能产生。用户实名制认证可通过线下方式（如通过自助终端读取用户证件）或线上方式（如通过金融交易机构对身份信息和银行账户信息进行验证）完成。

电子健康卡账户生命周期，包含账户的注册、个人信息变更、账户注销等，并支持账户黑名单机制。

电子健康卡账户绑卡信息包括：卡类型、卡号、绑卡时间等。

电子健康卡账户信息应在电子健康卡跨域主索引及跨域认证系统中进行索引（电子健康卡ID）注册。

6.2 二维码管理

电子健康卡管理信息系统应具备二维码管理功能，支持二维码生成及二维码验证。二维码生成及验证可基于软件实现，也可基于硬件实现，机构应结合自身使用场景和系统的实际情况选择安全可靠的二维码实现方案。

二维码管理功能应具备二维码的生成和验证的记录模块，提供对二维码生成和验证记录的分析和查询功能，提供对二维码使用过程的监控功能。

二维码管理功能应对动态二维码的生命周期进行管理。使用动态二维码时二维码管理功能应设置有效时间（超过有效时间后不可用），通过对时间的控制限制动态二维码的可用时间，从而保障动态二维码的使用安全。

6.2.1 二维码生成

二维码管理模块接收电子健康卡客户端应用软件或机构终端的二维码生成请求，依据电子健康卡二维码数据标准进行二维码生成。

二维码生成过程中，需要判断二维码生成类型。如果是静态二维码，由电子健康卡ID和静态标识符组成二维码。如果是动态二维码，由电子健康卡ID、动态标识符及有效时间密文组成二维码。

二维码生成流程如图 6.1所示：

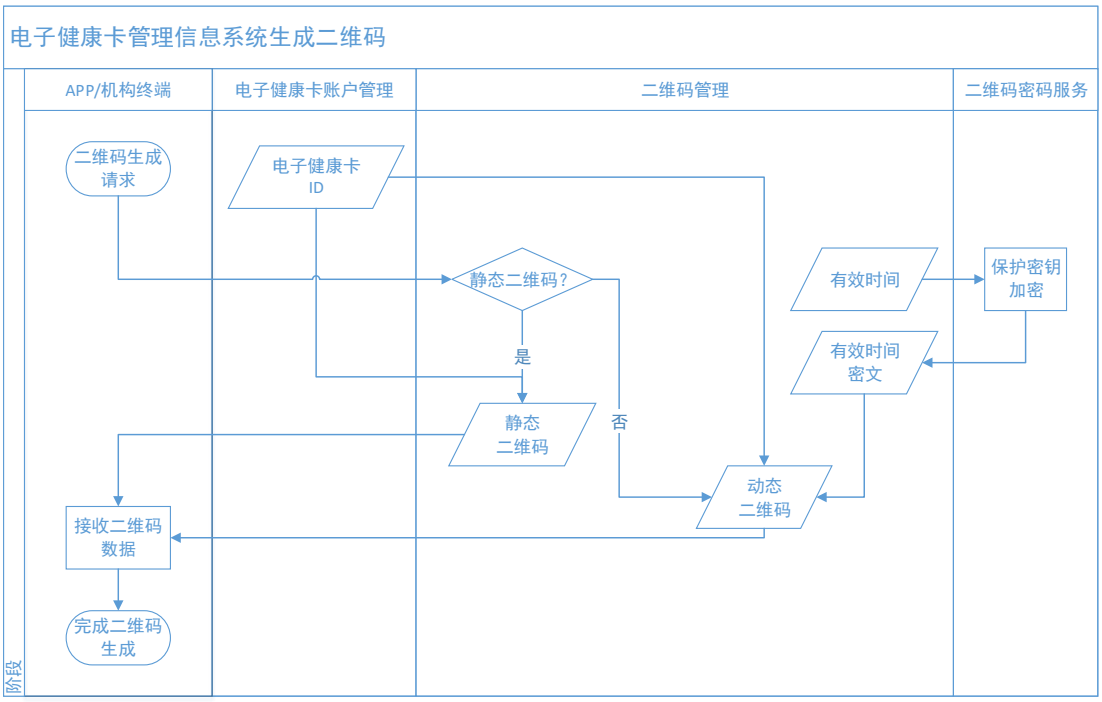


图 6.1 二维码生成流程

6.2.2 二维码验证

二维码管理模块接受二维码验证请求，根据电子健康卡二维码数据标准对识读终端上的二维码进行验证，并返回用户个人信息。本文中所称的二维码验证均是对二维码中数据内容的验证。

电子健康卡管理信息系统通过EHCIN判断该电子健康卡是否在本机构的系统中注册。如果EHCIN为本机构，则由本机构系统进行二维码验证。如果EHCIN非本机构，则通过调用电子健康卡跨域主索引及跨域验证系统对二维码进行跨域验证；跨域认证服务通过查询路由表，将验证信息发往EHCIN对应的机构进行验证；验证完成后，验证结果按照原路径返回，并在本机构系统中注册一张电子健康卡。

二维码验证时，通过密码服务解密电子健康卡ID，得到居民证件类型和证件号码，与账户管理中的证件类型和证件号码进行比对，识别使用电子健康卡的居民。动态二维码的有效时间密文通过密码服务解密，检查有效时间是否在许可时间使用范围内。

二维码验证流程如图 6.2所示：

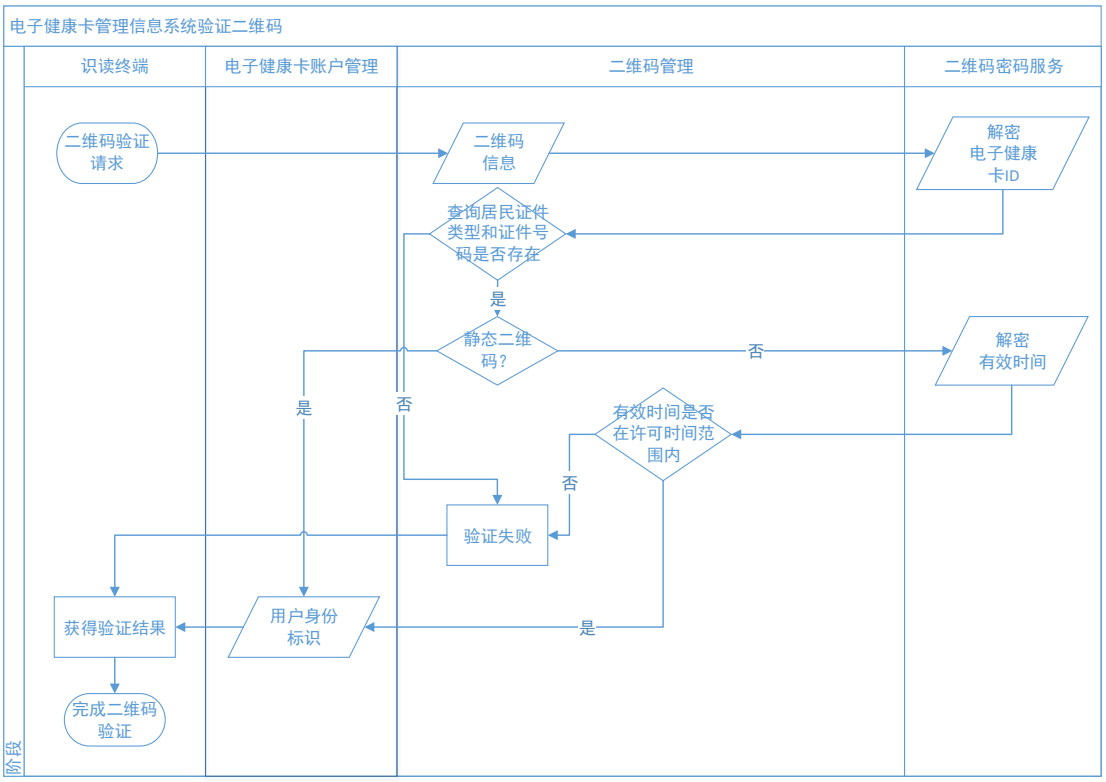


图 6.2 二维码验证流程

6.2.3 密码服务

电子健康卡管理信息系统密码服务功能区域包含密码模块，密码模块可以是硬件的密码机、密码卡。密码模块为电子健康卡管理信息系统的二维码管理模块提供密码服务，是电子健康卡管理信息系统的一部分，在物理环境上应与电子健康卡管理信息系统的其他功能模块同区域部署；密码模块仅对本电子健康卡管理信息系统的二维码管理模块提供密码服务，不向其他任何系统提供服务。

密码模块提供统一的主索引ID生成接口和电子健康卡ID接口，电子健康卡管理信息系统调用密码模块时，应符合“电子健康卡密码模块接口及卡管系统接入认证技术要求”中的要求。

6.3 机构接入管理

电子健康卡管理信息系统宜使用基于密码算法的认证技术，实现对接入组件的控制功能。采用密码算法进行接入控制时，宜采用符合GM/T 0028的三级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现签名认证服务。基于密码算法的认证技术实现方式可参见“电子健康卡密码模块接口及卡管系统接入认证技术要求V1.0”。

机构接入管理模块对接入机构的基本信息进行注册登记。机构接入管理模块具有信息登记、信息修改、信息删除、信息批量导入、黑名单等功能。

注册登记的信息应包括：组织机构代码、机构名称、机构类别、机构性质和机构接入日期等。表中所有项目均为必选项。

表 6.3 接入机构登记信息要求

序号	字段	可空	内容要求	示例
1	所属省份行政区划代码	N	6 位行政编码	
2	所属城市行政区划代码	N	地级市城市编码	
3	组织机构代码	N	医疗机构根据《WS 218 卫生机构（组织）代码》填写医疗机构执业许可证登记号；卫生管理机构等填写统一社会信用代码	例如：医疗机构执业许可证登记号（22 位）：73843029333030217A3591；统一社会信用代码（18 位）：11320982K13082661K
4	机构名称	N	医疗卫生机构名称	
5	机构等级	N	医疗机构等级编码表	
6	机构类别	N	医疗机构类别编码表	
7	机构性质	N	1：公立 2：民办 99:其他	
8	机构接入日期	N	机构接入的日期	2019/05/01

6.4 识读终端管理

识读终端应支持识读二维码:

——应保证二维码识读结果的机密性，避免二维码信息泄露；

——应保证二维码解析的准确性；

——应保证二维码识读解析结果表达的规范性；

——对于在原有 POS 等设备上进行扩展后具有二维码识读功能的设备还应遵守居民健康卡及国家金融行业相关标准；

——识读终端向后台服务端传输的信息中应包含识读终端相关信息。

识读终端管理模块对接入机构的终端等基本信息进行注册登记。登记的识读终端包括扫码枪、扫码墩、带扫码功能的自助服务终端等。识读终端管理模块具有信息登记、信息修改、信息删除、信息批量导入等功能。识读终端管理模块对接入的终端进行信息验证，保障接入的终端是经过注册登记的终端。

注册登记的信息应包括：终端编号、终端的名称、终端的版本、终端的使用单位、终端的开发单位等。表中所有项目均为必选项。

表 6.4 接入终端登记信息要求

序号	字段	可空	内容要求	示例
1	终端编号	N	由电子健康卡管理信息系统分配	见附录 D.2。
2	终端出厂序列号	N	通常为数字或字母形式	APOS20190718
3	终端的名称	N	终端内部名称	挂号自助终端
4	终端的用途	N	描述终端用途	用于患者自助进行挂号等操作
5	终端使用机构编码	N	医疗机构根据《WS 218 卫生机构（组织）代码》填写医疗机构执业许可证登记号；卫生管理机构等填写统一社会信用代码 （使用机构需要在机构接入管理中进行注册）	例如：医疗机构执业许可证登记号（22 位）：73843029333030217A3591；统一社会信用代码（18 位）：11320982K13082661K

6	终端使用机构名称	N	机构名称	挂号自助终端
7	终端的开发单位	N	工商注册名称	某某开发有限公司
8	终端接入日期	N	终端接入日期	2019/05/01

6.5 密码模块管理

密码模块管理对平台的密码模块基本信息进行注册登记。密码模块管理具有信息登记、信息修改、信息删除等功能。

注册登记的信息应包括：密码模块型号、密码模块生产商、密码模块序列号、密码模块接入日期、密码模块的系统地址等。

表 6.5 接入密码模块登记信息要求

序号	字段	内容要求	示例
1	密码模块编号	电子健康卡系统登记密码模块的编号	见附录 D.2。
2	密码模块型号	国家卫生健康委登记的型号	
3	密码模块生产商	国家卫生健康委登记的生产商信息	
4	密码模块序列号	硬件产品序列号	根据厂商具体的定义
5	密码模块接入日期	机构接入的日期	2019/05/01
6	密码模块的系统地址	密码模块的 IP 地址	如果有独立的 IP 地址就写明

6.6 数据接口要求

各建设单位的电子健康卡管理信息系统应与国家电子健康卡应用监测系统连接,保证电子健康卡管理接口、跨域查询接口的实时连通。

国家电子健康卡应用监测系统通过接口方式主动查询获取各地电子健康卡管理信息系统接入的APP、机构、识读终端等数据及电子健康卡使用情况数据，开展电子健康卡网络管理和用卡监测，接口应符合附录E。

6.7 数据审计

电子健康卡管理信息系统应具备数据审计功能，能够对用卡、发卡数据进行实时监测和统计，并提供用卡、发卡数据反查接口，通过该接口，实现用卡、发卡数据反查。

7 电子健康卡客户端应用软件接入与管理要求

7.1 客户端应用软件功能要求

电子健康卡应用的提供方可以基于现有的客户端应用软件,通过电子健康卡SDK调用电子健康卡API实现电子健康卡应用。

电子健康卡SDK应提供统一的电子健康卡管理信息系统的调用接口。采用电子健康卡SDK有助于实现健康卡应用的标准化。电子健康卡SDK应根据移动终端特性，提供支持原生开发语言及支持HTML5等不同实现方式的调用方式。

电子健康卡客户端应用软件向用户提供直接访问电子健康卡管理信息系统交互的接口，其主要功能有：

——电子健康卡用户注册；

——申请、下载、更新二维码；

客户端应用软件可以多种方式提供用户的身份鉴别,可采用:

——静态口令身份验证功能；

——动态口令身份验证功能；

——生物识别身份验证功能；

——基于密钥身份认证功能等。

客户端应用软件提供方可以根据业务、商业、运营环境等需求选择不同的身份鉴别功能或功能组合，也可以增加支持其他功能。

7.2 接入管理

客户端应用软件在接入前需提交《客户端应用软件接入信息登记表》，并按照《接入材料清单》要求提供相关接入材料。在正式接入前，应进行数据准确性联调测试，确认《客户端应用软件接入信息登记表》的数据与全国电子健康卡应用监测系统获取到的数据一致，测试通过后由客户端应用软件接入管理模块为其分配登记编号。

客户端应用软件接入管理模块应按照统一的编号规则（编号规则见附录D.2 电子健康卡接入组件入网编码规则），具备编号分配和管理、信息登记、信息修改、信息删除等功能，对接入的客户端应用软件进行注册管理，对违规的客户端应用软件进行暂停接入、整改后重新启用（详见材料二：电子健康卡质量控制与安全管理要求V2.2 3.2运行安全风险控制）。

电子健康卡客户端应用软件须在配置文件中保存分配的登记编号。Android版本应将编号保存在AndroidManifest.xml中，iOS版本应将编号保存在info.plist中。编号字段名称为“EHCI_KEY”。微信公众号、微信小程序、支付宝生活号、支付宝小程序等服务号应在域名下自建编号文件，名称为“EHCI_KEY”（无后缀名），编号采用utf-8编码保存在该文件中。如果一个客户端应用软件接入多个电子健康卡管理信息系统，则应在配置文件中同时保存多个编号，用英文逗号隔开。电子健康卡客户端应用软件应在电子健康卡展示页面的显著位置向用户提供该客户端登记编号的标识（见附录B图B.3 电子健康卡展示界面），编号应与配置文件中保持一致。

注册登记的信息见表7.1。表中可空列为N表示为必选项，Y表示可选项。

表 7.1 客户端应用软件登记信息要求

分类	参数	参数名称	类型	可空	参数说明	示例
资产信息	org_code	组织机构代码	String(32)	N	医疗机构根据《WS 218 卫生机构（组织）代码》填写医疗机构执业许可证登记号；卫生管理机构等填写统一社会信用代码（使用机构需要在机构接入管理中进行注册）	例如：医疗机构执业许可证登记号（22 位）：73843029333030217A3591；统一社会信用代码（18 位）：11320982K13082661K
	record_num	登记编号(EHCAPPID)	String(32)	N	由电子健康卡管理信息系统分配，编号规则见附录 D.2；	例如：1101A0056APPA0001

分类	参数	参数名称	类型	可空	参数说明	示例
					APP Android、APP iOS、公众号、服务号等每个应用种类均应分配唯一编号；	
	app_name	应用名称	String(50)	N	客户端应用软件显示给用户的名称	
	app_channel	应用种类	String(50)	N	该项为选择项，不可任意填写文本种类列表见附录 E7.7 应用种类一编码表	
	app_version	应用版本号	String(50)	N	版本号 X.Y 形式，应至少包含大版本和小版本 2 级	例如：1.2 或者 1.2.1
	app_category	应用服务种类（可多选）	String(50)	N	该项为多选项，不可任意填写文本种类列表见附录 E 中 7.8 应用种类二编码表；	
	app_package	应用包名	String(50)	Y	仅 APP 填写，app 应用包名	例如：com.ehealth.hospital
	dev_unit	开发单位名称	String(50)	N	工商注册名称	填写全称
	use_unit	应用运营机构名称	String(50)	N	应用的运营责任承担主体	
	use_unit_type	运营机构类型	String(10)	N	A 卫健委；B 医院；C 公共卫生机构；D 基层卫生机构；E 政府其他部门；F 第三方机构；X 其他	A
	use_unit_people	运营机构联系人	String(50)	N		
	use_unit_phone	运营机构联系方式	String(50)	N		
	use_unit_mail	运营机构邮箱	String(50)	N		
	copyright_no	应用著作权编号	String(50)	Y	应用的著作权登记号	2021SR***035
	icp_no	应用 ICP 备案编号	String(50)	Y	应用的 ICP 备案编号	
	djbh_no	应用等保报告编号	String(50)	Y	应用取得的等保报告编号	
状态信息	record_time	应用接入日期	String(8)	N	接入电子健康卡系统时间，分配接入编号的日期，格式：年月日 yyyyMMdd	例如：20201001
	launch_time	应用上线日期	String(8)	Y	应用正式上线日期，格式：年月日 yyyyMMdd	例如：20201001
	app_url	应用地址	String(100)	N	APP 填写下载地址 公众号、小程序等填写域名地址	例如：https://itunes.apple.com/cn/app/id1398635899?mt=8

分类	参数	参数名称	类型	可空	参数说明	示例
	img_url	应用 logo 地址	String(100)	N	公众号、小程序、APP 的可以进行引用的 logo 地址，	例如：https://应用域名/icon.png
	release_channel	发布渠道	String(50)	Y	仅 APP 填写；该项为选择项，不可任意填写文本 渠道分类见附录 E 中 7.9 发布渠道编码表	
	erhc_system	接入的卡管节点名称	String(50)	N	由电子健康卡管理系统自动关联填写	如北京西城管理节点
	erhc_system_record_no	卡管节点入网编码(EHCIN)	String(50)	N	由电子健康卡管理系统自动关联填写	1101A0056
	online_status	应用在线状态	String(5)	N	由电子健康卡管理系统判断应用在线联通状态 1-联网 2-未联网 3-停用	1

7.3 安全要求

电子健康卡客户端应用软件应符合下列要求：

——客户端应用软件应提供数据有效性校验功能，软件的下载、安装与更新时应采用安全防护措施；

——应对客户端程序进行签名，标识客户端程序的来源和发布者，保证客户所下载的客户端程序来源于所信任的机构；

——客户端宜采用防逆向工程保护措施，如客户端可采取代码花指令、反调试、代码混淆等技术手段，防范攻击者对客户端的反编译分析；

——客户端启动和更新时，宜进行真实性和完整性校验，防范客户端被篡改；

——应用软件与后台系统应具备合法性认证机制，并具备记录所有用户访问日志的功能；

——应采用安全的密码输入方式；

——应对数据进行安全存储，防止敏感信息泄露；

——客户端应从木马病毒防范、信息加密保护、运行环境可信等方面提升安全防控能力；

——电子健康卡 SDK 开发商应对电子健康卡 SDK 的调用提供安全指导手册；

——采用电子健康卡 SDK 的客户端应用软件开发商应按照电子健康卡 SDK 开发商的安全指导进行调用；

——电子健康卡客户端应用软件（或机构）应向电子健康卡管理信息系统进行接入登记，宜采用电子健康卡管理信息系统接入层认证方案接入电子健康卡管理信息系统，详见“电子健康卡密码模块接口及卡管系统接入认证技术要求”。

——应完善客户端应用软件的安全风险防护措施，加强移动应用资产管理、安全风险管理和个人信息保护管理，对发现的漏洞和潜在的风险及时采取补救措施，对于仿冒、钓鱼类应用的出现及时通知应用渠道管理方进行下架处理。

——应建立安全风险动态监测管理机制，通过主动、持续、动态的风险业务识别、侦测和分析，达到风险识别、预警、处置的风险闭环控制。

——应加强个人健康生理信息保护措施，遵循合法、正当、必要的原则，明示收集使用信息的目的、方式和范围，并经用户同意，不可超范围收集个人信息。

8 电子健康卡运行可靠要求

8.1 运行可靠性

为保障电子健康卡平台安全平稳运行，建设单位应确保电子健康卡在使用期间对于电子健康卡注册、生成二维码和验码功能的安全稳定运行，尤其是业务高峰期，保障7×24小时不间断运行。系统新版本上线后若发现故障，应能够快速回滚，确保数据不丢失。

电子健康卡管理信息系统要对内部接口和外部接口进行分类管理，在外部接口故障时，可通过停止或减少外部接口调用等方式避免影响系统稳定运行。如遇突发情况可采取限流、排队、服务端缓存、手机客户端缓存、内容分发网络（CDN）、用户刷新频率限制等技术措施，加强应对突发尖峰流量冲击的能力。

8.2 承载能力

电子健康卡管理信息系统应根据部署地常住人口与系统历史最大并发数等因素，评估确定合理容量，具备在容量不足时进行快速扩容的能力，当系统实际并发流量超过设计容量70%时应进行扩容。

9 电子健康卡安全要求

9.1 通用要求

系统安全应符合GB/T 22239-2019和GB/T 39786-2021中第三级要求。

系统应采用SM2、SM3、SM4国产密码算法，采用国密标准的VPN、SSL/TLS。

系统应支持7x24小时正常运行。

系统间数据传输应采用密码技术保证传输数据的保密性、完整性、不可抵赖性。

9.2 身份认证要求

电子健康卡管理信息系统应基于数字证书进行用户访问强身份鉴别，从而降低系统安全风险。数字证书宜采用基于国密算法的第三方数字证书，实现电子健康卡管理信息系统电子认证服务体系。实现方案详见附录F 电子健康卡管理信息系统身份认证方案。

9.3 实名认证要求

医疗卫生机构应对注册电子健康卡的居民进行实名认证，需在窗口注册、自助终端注册、移动客户端应用软件注册等不同渠道设置适当的实名认证方案，并满足以下要求：

（一）医疗卫生机构自主或委托合作机构以面对面方式核实居民身份，应对居民有效的实名身份证件进行确认。

（二）医疗卫生机构可以非面对面方式核实居民身份。应通过至少一个合法安全的外部渠道进行身份基本信息验证。居民身份基本信息外部验证渠道包括但不限于政府部门数据库、商业银行信息系统、商业化数据库等。其中，通过商业银行验证个人客户身份基本信息的，应为Ⅰ类银行账户或信用卡。

9.4 电子健康卡管理信息系统安全要求

电子健康卡管理信息系统涉及到居民个人信息，必须加强访问控制，建立完善的日志系统。

——根据“业务需要”和“最小权限”原则，严格控制访问，任何人都只能访问其开展业务所必需的信息，并且只能够获得访问所必要的最少权限。

——应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

——记录具有管理员权限对系统的身份识别和验证机制（包括但不限于创建新账户、提升权限等）进行使用和更改，并对应用程序账户进行任何更改、增加、删除的行为。

——记录分配有管理权限的任何个人所做的所有操作。

——记录所有单个用户对系统内敏感数据的访问。

——为所有电子健康卡系统平台建立统一的时间服务，实现不同系统间的时钟同步。

电子健康卡管理信息系统对外提供服务，其必须建立安全机制及策略，保障系统安全及信息交互安全。

——建立安全访问机制，应通过访问控制列表对系统资源实现允许或拒绝用户访问；

——攻击防范，抵御常见的SQL注入、跨站脚本、网页挂马等攻击手段；

——API调用安全，应对API的调用进行授权控制，仅允许合法的接入方调用API；

——通信完整性，应采用约定通信会话方式的方法保证通信过程中的数据完整性；

——系统容错，应提供数据有效性功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；

——数据加密保护，应对敏感信息通过密码算法进行加密存储；

——数据备份及恢复，应能够对重要数据进行备份和恢复。

电子健康卡管理信息系统需同时接收不同机构上传的信息，处理大量并发验证。

——应确保系统的并发处理能力，满足既定的业务需要。

——应确保系统的响应速度，在有效时间内返回认证结果。

——应定义系统的RTO与RPO，并满足相应能力。

9.5 电子健康卡密码模块部署安全要求

电子健康卡密码模块是电子健康卡安全保障的重要组成部分。电子健康卡密码模块在研发阶段和应用阶段应分开管理，保证电子健康卡密码应用的安全。

在研发阶段，结合项目实际情况，应设立密码模块接口开发专职人员，主要负责密码模块接口调用，以及为电子健康卡其他研发人员提供方便易用接口封装。

在应用阶段，密码模块部署时应满足如下条件：

——硬件设备物理部署符合国家对密码机部署的标准。

——密码模块应位于密码机网络安全隔离区，划分逻辑隔离控制网络访问权限。

——密码模块部署时应与电子健康卡管理信息系统同区域物理部署。

——密码模块应对电子健康卡管理信息系统进行安全接入认证。

——密码机可支持多机部署，应满足以下要求：

——开发密码机前置代理服务程序，避免泄露密码机 IP 地址和端口等信息。

——密码机内置网络安全白名单，只允许密码机前置代理服务程序调用密码机接口。

——密码机前置代理程序指定调用者白名单，只允许电子健康卡服务程序访问。

——密码机前置代理服务支持负载均衡并结合密码机本身提供的负载方案，实现完整负载均衡方案，可以做到电子健康卡无感知动态扩容密码机。

——前置代理服务程序增加对密码机调用接口细粒度权限控制功能，可以实现对生成主索引ID、生成电子健康卡、解密电子健康卡、校验时间有效性等接口的细粒度控制功能。提供此功能的目的在于电子健康卡系统平台由多个功能组件构成，不同组件根据业务划分不同，按照最小化原则分配密码机调用权限。

——密码机权限管理提供接口调用日志审计功能，可回溯密码机使用日志信息。

——多台密码机的部署如图 8.1所示。

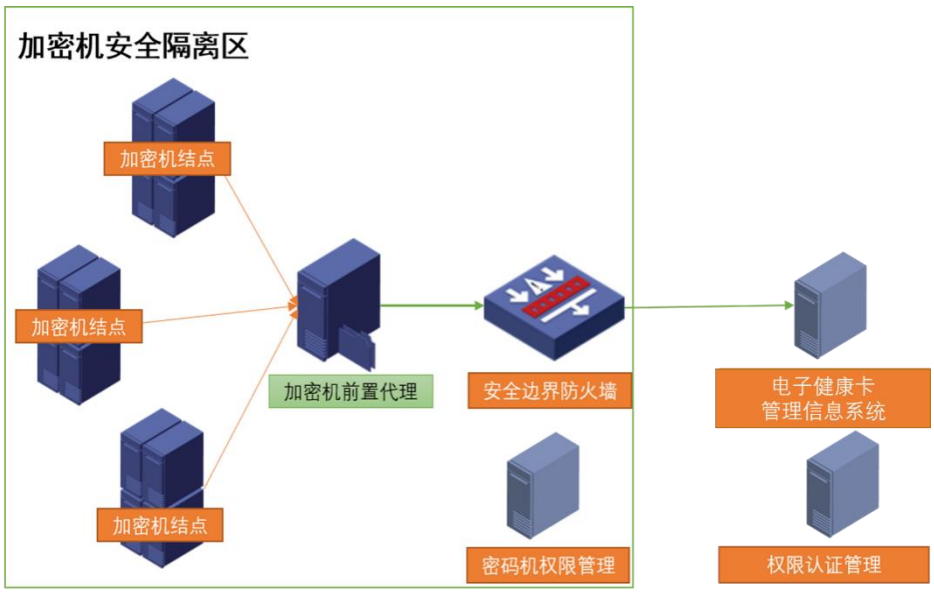


图 8.1 电子健康卡密码机部署示意图

9.6 网络通信安全要求

网络通信应符合下列要求：

——应在医疗卫生机构、金融交易机构与电子健康卡管理信息系统之间通过专线或VPN进行通信，保护数据通信安全；

——应在客户端与服务器之间建立安全的信息传输通道，通过公开网络进行数据传输时，应进行双向认证，例如使用数字证书；

——如使用SSL/TLS协议，应使用相对高版本的协议，取消对低版本协议的支持。

9.7 二维码技术应用要求

在电子健康卡应用中使用的二维码技术应确保具有访问权限的使用者具备唯一的身份标识 ID。使用的二维码技术应该具备一般用户验证机制、重置验证机制，并且对验证信息进行保护，对登录失败次数设置合理上限。

在电子健康卡应用中使用的二维码技术应确保存储信息的安全性，且不应存储敏感信息。

在电子健康卡应用中，应对传输的数据进行保密性保护，并具备鉴别机制，还应确保接收信息或发送信息的主体在数据交换期间能获得证明该信息发送或接收的证据。

9.7.1 数据要求

——输入数据信息转成一个或多个二维码，被识读解码后应完全重现输入数据信息，不得出现任何差异。

——二维码的表达必须符合相应的国家标准规范。输入数据信息转成一个或多个二维码，被任何符合国家标准规范的二维码识读设备识读后的数据信息必须具有唯一性。
——二维码纠错等级应选用可恢复码字比例不小于15%的等级。

9.7.2 表现要求

——二维码应与居民健康卡标识（LOGO）相结合，展现居民健康卡品牌性。
——二维码应表现在平面介质上，不得扭曲、变形、破坏。
——二维码应完整表现，且二维码外围空白区应符合码制要求。
——二维码可表现在主动发光表面介质，包括但不限于LCD、LED屏幕等，半主动发光表面介质，包括但不限于光学投影幕墙等，和被动反射表面介质，包括但不限于打印纸质材料、电子墨水屏幕等。
——二维码主体应采用黑白或深浅反差尽量大的两种色块表示。
——对于被动反射表面介质，要求PCS值不小于30%。
——对于被动反射表面介质，最高表示精度不应超过0.254mm（10mil）。
——对于主动、半主动发光表面介质，最高表示精度不应超过0.381mm（15mil）。
——二维码应根据需求生成PNG/JPG/BMP等格式。

9.7.3 识读要求

——对于被动反射表面介质，最高识读精度应达到0.254mm（10mil）。
——对于主动、半主动发光表面介质，最高精度应达到0.381mm（15mil）。
——对于一个二维码，申请到展示的时间应不超过3秒，识读时间应不超过1秒。
——如果二维码交易过程一次识读步骤中需识读多个二维码，全部识读时间应不超过5秒。
——对于识读解码能力范围内的标准测试版，出错率应小于0.01%。

9.7.4 安全要求

——二维码的产生过程必须由保护密钥参与运算，二维码的验证过程其核心就是通过保护密钥验证其数据。
——应采取安全技术对二维码中包含的敏感信息进行加密处理。
——应确保生成二维码的软件、设备的安全性，防止生成的二维码携带病毒、木马等数据或者链接，防止生成的二维码被篡改、替换。
——动态二维码应根据风控能力设置有效时间。
——应采用有效措施，确保二维码信息的真实性、完整性、一致性和抗抵赖性。
——在电子健康卡应用中使用的二维码技术应确保具有访问权限的使用者具备唯一的身份标识ID。
——使用的二维码技术应该具备一般用户验证机制、重置验证机制，并且对验证信息进行保护，对登录失败次数设置合理上限。
——在电子健康卡应用中，应对传输的数据进行安全性保护，并具备鉴别机制，还应确保接收信息或发送信息的主体在数据交换期间能获得证明该信息发送或接收的证据。

9.8 识读终端安全要求

识读终端应保证识读结果的机密性，避免二维码信息泄露。

二维码解析时应满足以下要求：

——应对二维码完整性进行校验；

——应对二维码的真实性进行校验；

——应识别病毒、木马等恶意数据，保障交易的安全性。

识读终端如果具有金融交易的 PIN 输入相关场景，应具备一定的物理、逻辑安全机制，如应具备入侵检测机制，防止 PIN 输入过程被监听，可安全地存储敏感信息，具备完整的密钥体系等。在 PIN 输入设备和非接触式读卡器间传输 PIN 相关信息时，应有效地保护所传输的数据。PIN 输入设备应满足金融行业相关规范的要求。

应采取技术手段实现二维码业务的识读终端、通信网络与其他业务系统实现隔离。

10 电子健康卡系统平台管理要求

10.1 通用要求

10.1.1 系统建设管理

——应以书面的形式说明系统部署的边界、系统建设的方法和理由。

——应组织相关部门和有关安全技术专家对系统建设的合理性和正确性进行论证和审定。

——应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。

——应确保信息安全产品采购和使用符合国家的有关规定。

——应确保密码产品采购和使用符合国家密码主管部门的要求。

10.1.2 系统开发管理

——自行开发时，应确保开发环境与实际运行环境物理分开，测试数据和测试结果受到控制，并确保在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。

——外包软件开发时，应在软件交付前检测软件质量和其中可能存在的恶意代码，并要求开发单位提供软件设计文档和使用指南。

10.1.3 工程实施管理

——应指定或授权专门的部门或人员负责工程实施过程的管理；

——应制定工程实施方案控制安全工程实施过程。

10.1.4 测试验收

——制订测试验收方案，并依据测试验收方案实施验收，形成测试验收报告；

——应进行上线前的安全性测试，并出具安全测试报告。

10.2 电子健康卡管理信息系统管理

电子健康卡管理信息系统是电子健康卡的核心系统，为确保电子健康卡管理信息系统的运营安全，应建立安全管理制度。

10.2.1 资产管理

——应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。

——应确保介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。

10.2.2 网络和系统安全管理

——应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限。

——应指定专门的部门或人员进行账号管理，对申请账号、建立账号、删除账号等进行控制。

——应建立网络和系统安全管理制度，对安全策略、 账号管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定。

——应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等。

——应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。

10.2.3 配置管理

——应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。

10.2.4 变更管理

——应明确系统变更需求，变更前根据变更需求制定方案，变更方案经过评审、审批后方可实施。

10.2.5 备份与恢复管理

——应识别需要定期备份的重要业务信息、系统数据及软件系统等。

——应规定备份信息的备份方式、备份频度、存储介质、保存期等。

——应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。

10.2.6 安全事件处置

——应报告所发现的安全弱点和可疑事件。

——应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等。

——应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。

10.3 电子健康卡管理信息系统接入管理

为保证接入电子健康卡管理信息系统的第三方不会引入系统风险，电子健康卡管理信息系统的运营方应对接入方提出安全和管理要求。应包括：

——制定接入方接入的管理办法和相关流程。

——对接入方的机构信息、资质信息等进行备案管理。

——监督接入方的系统安全状况，如检查接入方的系统是否具有安全性证明材料，检查接入方的客户端应用软件是否具有安全性报告。

——制定接入方的安全评价标准。

附录A　（资料性）网络架构图

附录 A 给出了电子健康卡服务节点的基本网络安全防护架构参考图。其中：

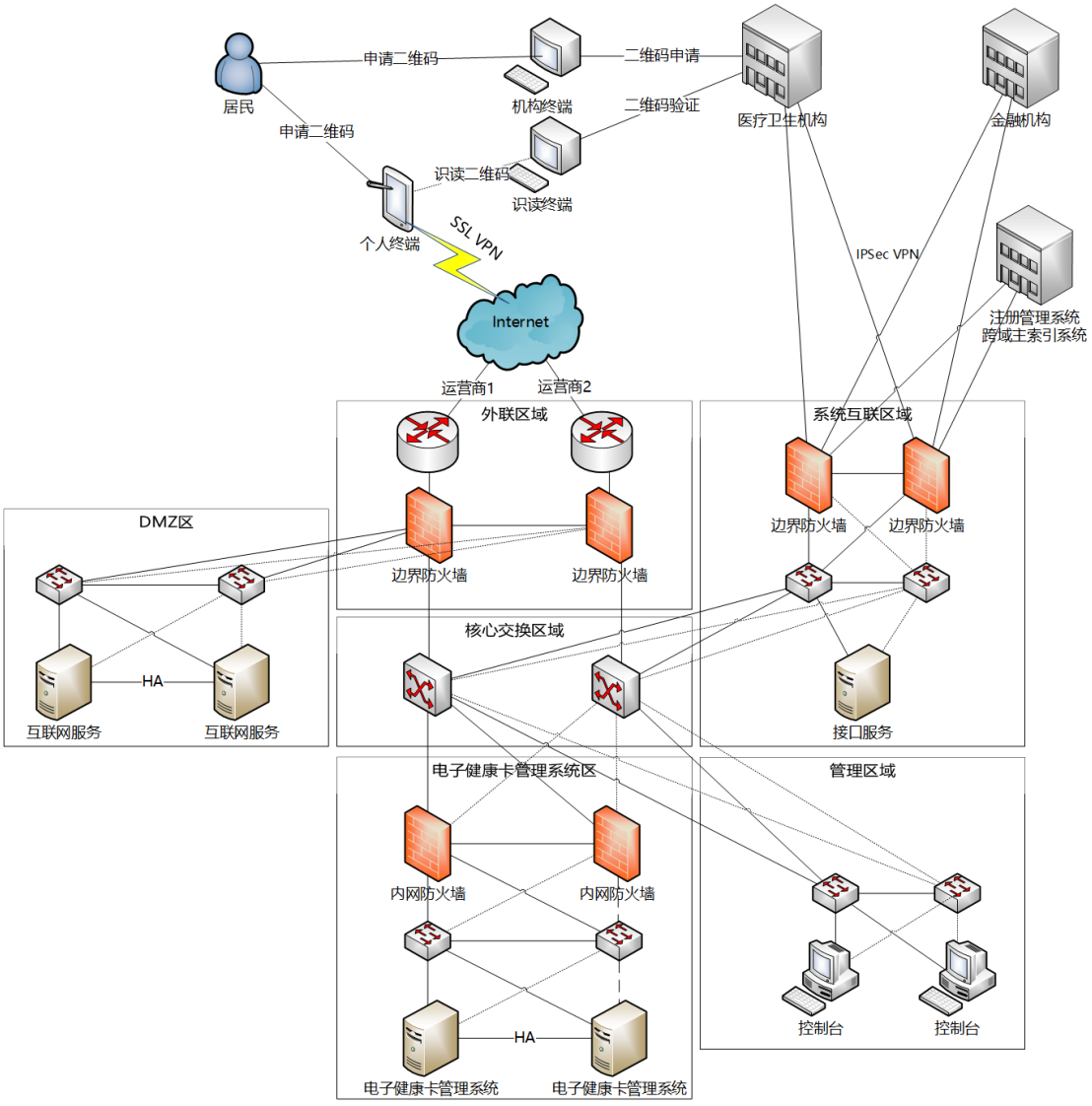
——外联区：主要处理外部访问的区域。

——DMZ 区：是一个公布信息的区域，通过互联网接入的外部客户可以访问该区域。

——电子健康卡管理信息系统区：是电子健康卡管理信息系统的部署区域，处理电子健康卡业务逻辑。

——管理区域：主要负责管理设备的接入。

——系统互联区域：主要处理电子健康卡管理信息系统与医疗机构系统、金融机构系统互联的区域。



图A.1　网络架构图

附录B　（规范性）电子健康卡展示界面及卡面规范

本部分给出了电子健康卡的展示界面及卡面规范的要求。建设单位应遵循本附录进行电子健康卡卡面展示和卡面设计。

B.1　电子健康卡客户端界面要求

卡面应包括以下要素：国家电子健康卡标识及图案、二维码图案、用户姓名（掩码显示：第 2 个字采用*显示）、证件号码（掩码显示：除前 4 位和后 4 位，均采用*显示）、发卡机构名称、监制机构。

图 B.1 卡面参考布局

图 B.2 卡面尺寸（单位：px/像素）

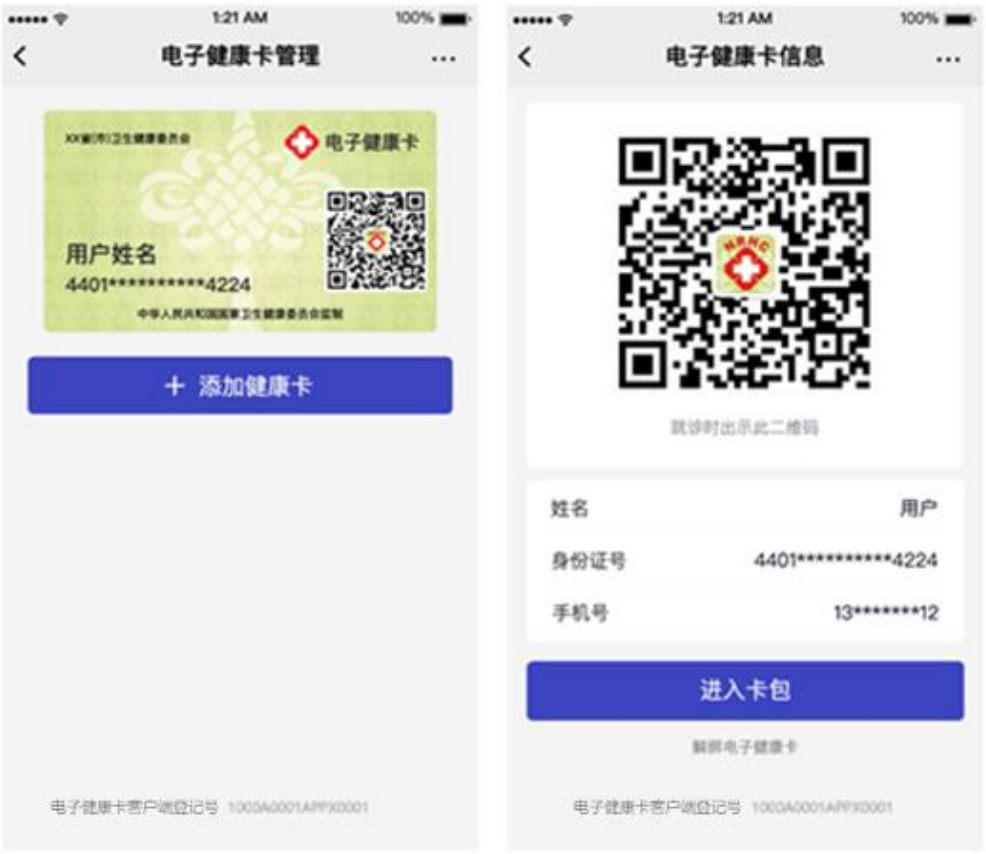


图 B.3 电子健康卡展示界面

表 B.1 卡面参数布局参数（单位：px/像素）

参数		规格及要求
卡面	卡面宽度	620px
	卡面高度	350px
	卡面圆角	10px
发卡机构标识区	“省（市）级卫生健康行政管理部门名称”字体	苹方中黑体（18Px）
	“省（市）级卫生健康行政管理部门名称”区域左边沿到卡的左边沿的距离	34px
	“省（市）级卫生健康行政管理部门名称”区域上边沿到卡的上边沿的距离	32px
	“省（市）级卫生健康行政管理部门名称”区域高度	25px
持卡人个人信息区	“姓名”字体	苹方中黑体（36Px），掩码显示：第 2 个字采用*显示
	“证件号码”字体	苹方中黑体（30Px），掩码显示：除前 4 位和后 4 位，均采用*显示
	“姓名”、 “证件号码”左边沿到卡的左边沿的距离	35px
	“姓名”上边沿到卡的上边沿的距离	202px

参数		规格及要求
	“姓名”、 “证件号码” 的行间距	2px
	“姓名、证件号码”字色值	2B2B2B
二维码区	二维码区域宽度	162px
	二维码区域高度	162px
	二维码描边	4px
	Logo 宽度	44px
	Logo 高度	44px
	Logo 圆角	8px
	Logo 描边	4px
	备注：logo 图片的大小不应影响二维码的译码	
监制机构区	“监制机构”字体	苹方中黑体（18 Px）
	“监制机构”字间距	0
	“监制机构”下边沿距卡的下边沿的距离	18px
	“监制机构”水平方向	与电子健康卡的卡面区域内居中
	“监制机构”左边沿到卡的左边沿的距离	142px
	“监制机构”上边沿到卡的上边沿的距离	309px
电子健康卡标识区	电子健康卡图片标识红色部分色号	ED1C24
	“电子健康卡及标识”区域	卡片右上区域
	“电子健康卡图片标识”上边沿距卡上边沿	23px
	“电子健康卡图片标识”左边沿距卡左边沿	380px
	“电子健康卡”文字上边沿距卡上边沿	29px
	“电子健康卡及标识”子左边沿距卡左边沿	443px

B.2 自助终端界面要求

自助终端显示就诊卡时，可同时展示电子健康卡和其他类型就诊卡。电子健康卡的展示位置应位于就诊卡页面的首位。其他类型的就诊卡宜置于二级菜单。

附录C　（资料性）电子健康卡时钟同步系统部署方案

由于电子健康卡系统平台主要的功能为发放电子健康卡、使用电子健康卡、管理电子健康卡，在发放、使用和管理过程中，电子健康卡出现的时间非常重要。为保证不同区域部署的电子健康卡系统平台在统一时间下提供服务，形成完整的时间服务链条，附录 C 给出了一种电子健康卡时钟同步系统的部署方案。

在电子健康卡系统平台的主要节点（如国家卫生健康委、省卫健委）部署两套主时钟服务器，每台主时钟服务器能各自接收北斗信号、GPS 信号进行授时或连接国家授时中心进行授时，且两套主时钟服务器互联热备信号，获取国家时间源。在各地市卫健委部署从时钟服务器，从时钟服务器通过时钟同步系统能同时接收主时钟发送的两路时间同步信号，具有内部时间基准，并按照要求的时间准确度向外输出时间同步信号和时间信息，以完成电子健康卡的时间链条。参考部署网络如图 C.1 所示：

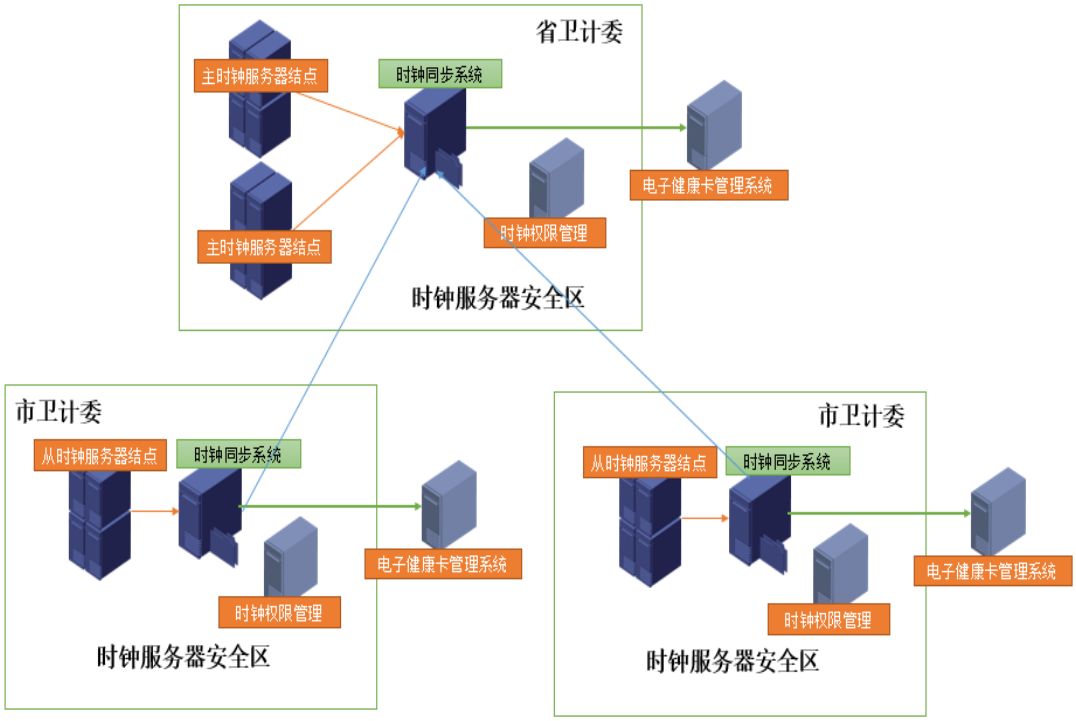


图 C.1 省-市两级电子健康卡时钟服务器统一部署架构图

附录D　（规范性）电子健康卡网络编码规则

本部分给出了电子健康卡管理信息系统以及接入电子健康卡管理信息系统的电子健康卡客户端软件、信息系统、自助终端等接入组件的编码规则。

D.1　电子健康卡管理节点入网编码规则

电子健康卡管理节点采用唯一的编码标识其在网络中的身份，由国家委统一分配。电子健康卡管理节点入网编码即EHCIN（电子健康卡管理信息系统标识号）。标识号由字母数字混合码组成，标准位数共9位，组成顺序为地区省代码、市代码、主管单位类别、备案顺序流水号。

组成说明如下：

一级类目码为2位数字码，使用地区省代码，标准以国家发布为准；

二级类目码为2位数字码，使用地区市代码，标准以国家发布为准，如无二级类目码使用00补齐；

三级类目码位1位字母码，表示主管单位类别，分类为A卫健委；B医院；C公共卫生机构；D基层卫生机构；E政府其他部门；F第三方机构；X其他。

四级类目码为4位数字码，顺序编号，流水号标准为四位，如：0001~9999。

表 2 电子健康卡管理节点入网编码结构

组成	地区省、市代码		类别	流水号
名称	一级类目码	二级类目码	三级类目码	四级类目码
类型	数字码	数字码	字母码	数字码
长度	2 位	2 位	1 位	4 位
标准	省代码	市代码	A、B、C、D、E、F、X	0001~9999

电子健康卡管理信息系统的建设单位应在电子健康卡管理信息系统中录入电子健康卡管理信息系统编号，编号一经录入后不能进行变更。

D.2　电子健康卡接入组件入网编码规则

电子健康卡接入组件包括客户端应用软件、信息系统、识读终端等，由各卡管自主分配。组件采用唯一编号（EHCAPPID）。登记编号（EHCAPPID）由字母数字混合码组成，标准位数共17位，组成顺序为电子健康卡管理信息系统编号（EHCIN）、接入组件类别、顺序流水号。

组成说明如下：

一级类目码为9位，即申请接入的电子健康卡管理信息系统项目编号。

二级类目码为3位字母码，客户端应用软件类别，分类为APP代表应用软件；GZH代表公众号；XCX代表小程序、SHH生活号；FWH代表服务号；QTH代表其他号；ZZJ代表自助机；XXT代表信息系统；STM代表识读终端；CRP代表密码模块。类别编码由国家统一维护，各地卫健委有新增类别需求的可与国家卫生健康委联系。

三级类目码位1位字母码，表示主管单位类别，分类为A卫健委；B医院；C公共卫生机构；D基层卫生机构；E政府其他部门；F第三方机构；X其他。

四级类目码为4位数字码，顺序编号，流水号标准为三位，如：0001~9999。

表 3 接入组件编号码位结构

组成	电子健康卡管理信息系统编号	类别	主管单位类别	流水号
名称	一级类目码	二级类目码	三级类目码	四级类目码
类型		字母码	字母码	数字码
长度	9 位	3 位	1 位	4 位
标准	EHCIN	APP、XCX、SHH、GZH、FWH、QTH、ZZJ、XXT、STM、CRP	A、B、C、D、E、F、X	0001~9999

附录E　（规范性）国家电子健康卡应用监测系统数据采集标准规范

1　范围

本文适用于电子健康卡管理中心管理人员、电子健康卡监测管理人员、电子健康卡卡管系统厂商技术人员阅读，指导国家、省级、市级及机构电子健康卡管理中心开展本级电子健康卡管理信息系统和电子健康卡监管平台的建设 规范化建设，并实现与电子健康卡监测平台的互联互通。

本文详细列出相关电子健康卡监测平台数据采集的改造流程和注意事项，提供相应的接口规范和要求。

2　监测系统架构

2.1　平台系统结构

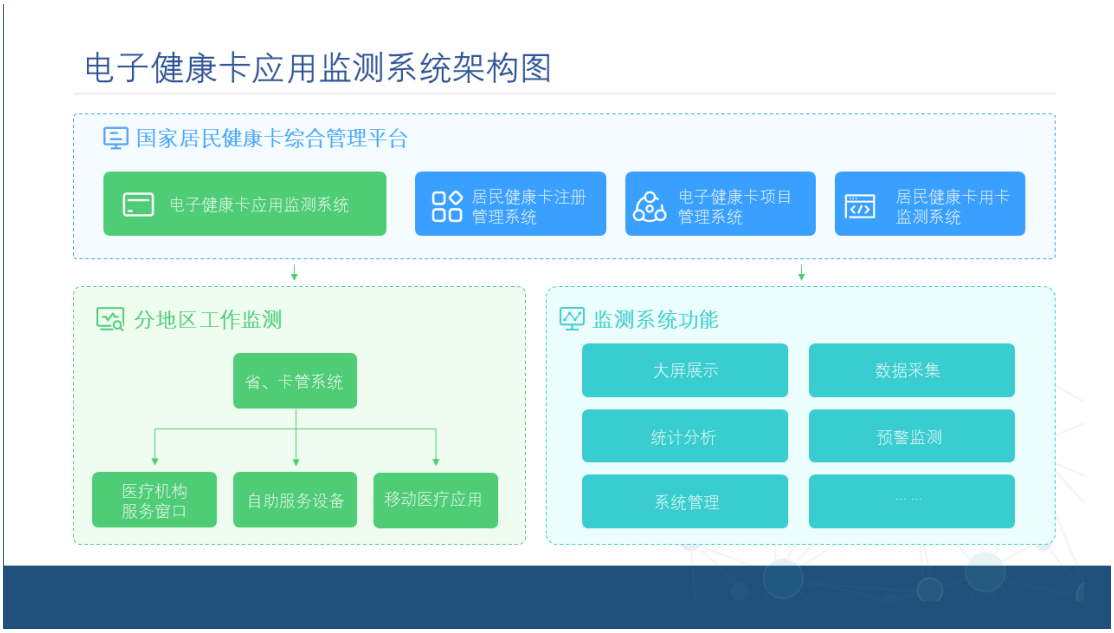


图 10.1 监测平台系统结构

2.2　平台网络方案

2.2.1正式环境网络连接

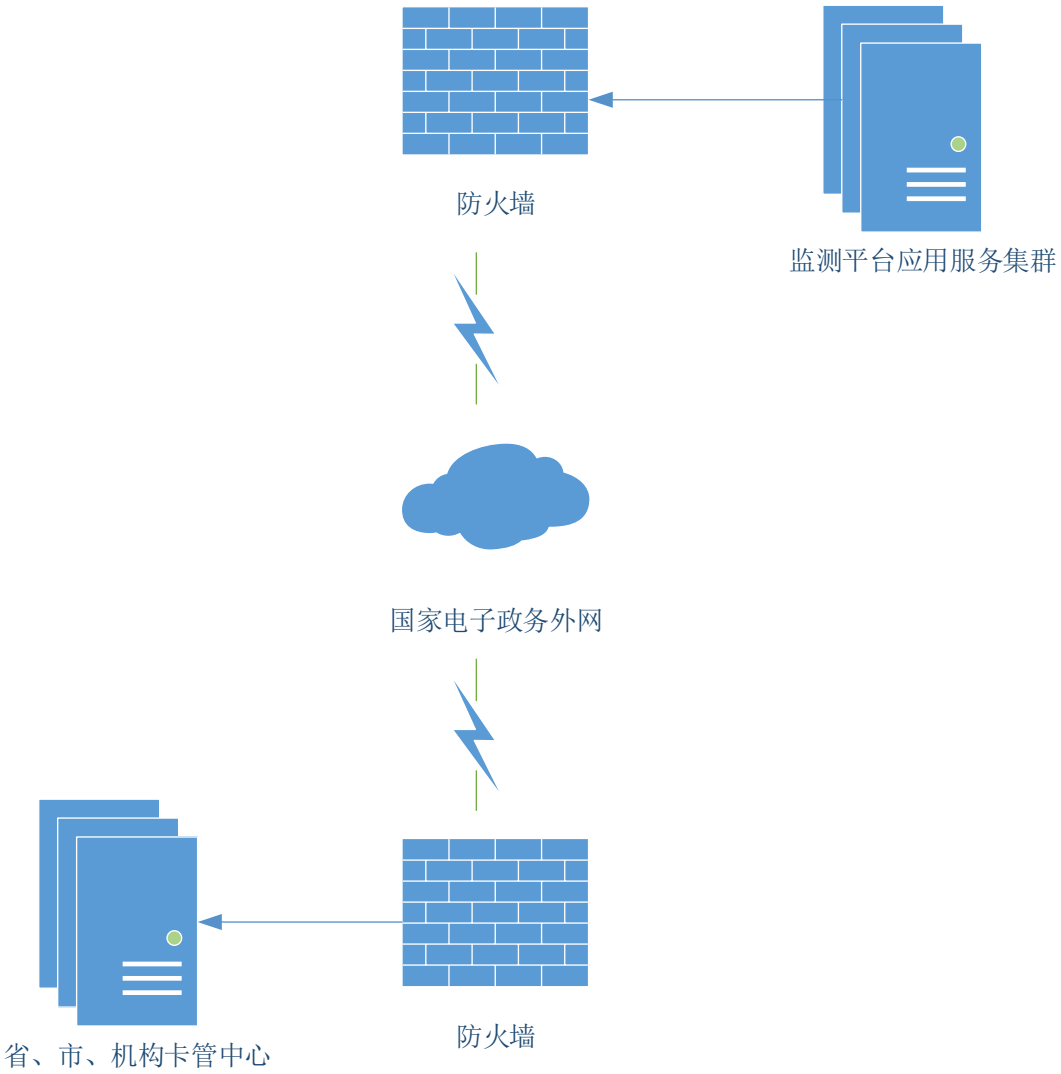


图 10.2 监测服务平台正式网络连接

2.2.2测试环境网络连接

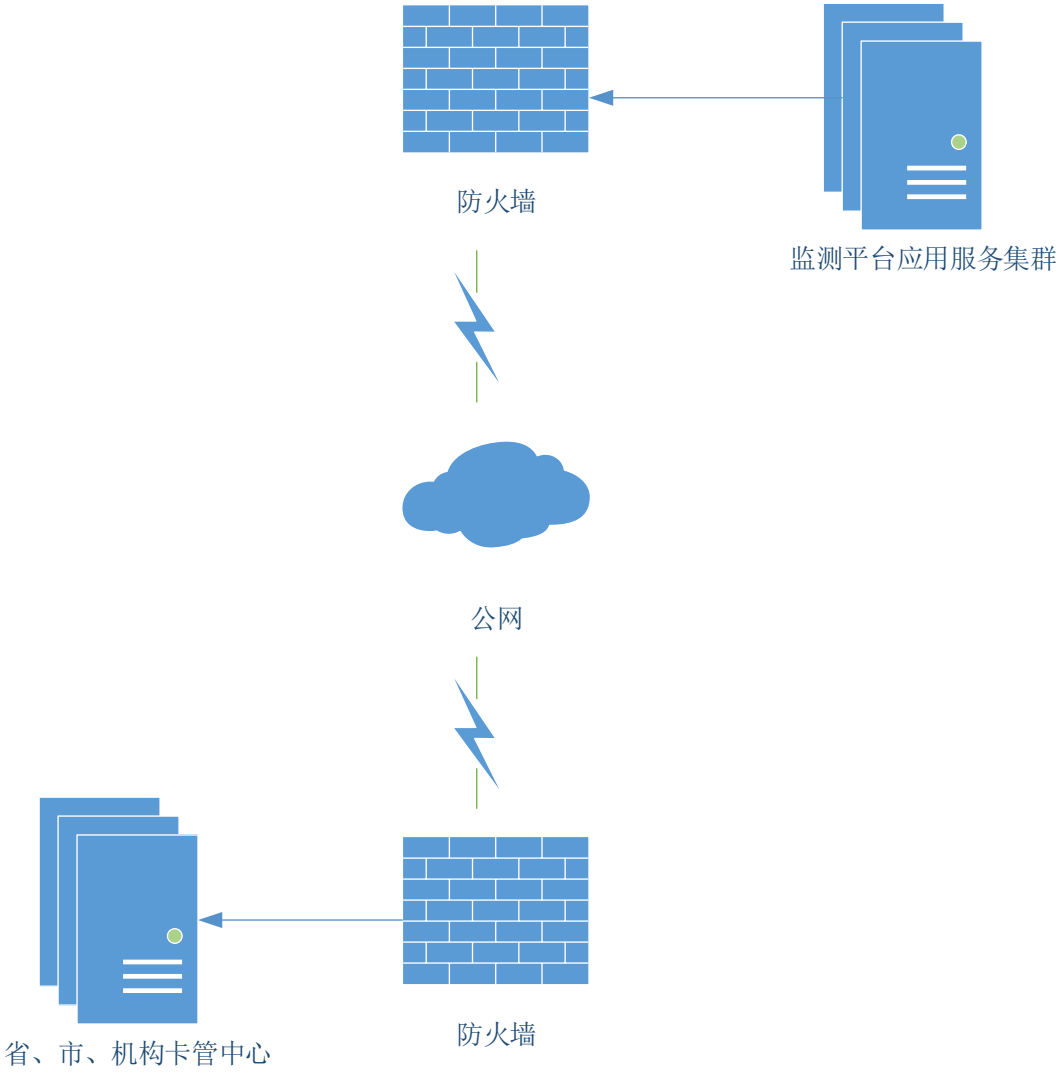


图 10.3 监测服务平台测试网络连接

3 监测数据采集方案

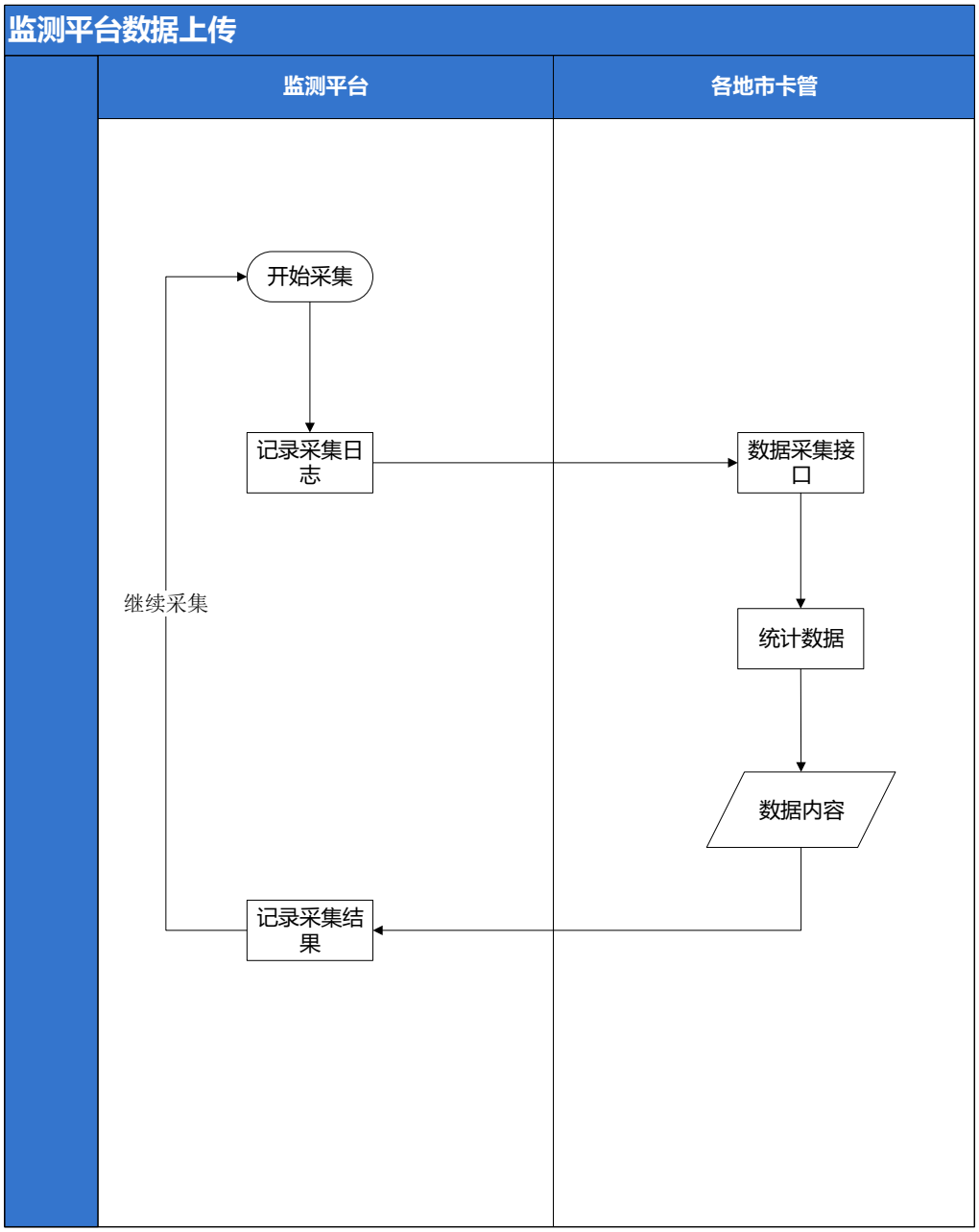
3.1 改造内容概述

为了配合国家卫生健康委对电子健康卡业务监测，对电子健康卡运行效果分析，各省市级卡管平台需要配合改造提供数据采集接口，改造内容主要可以分为以下两个部分：

各省市级卡管平台按该标准规范提供数据接口。

由于个别省份存在省市级电子健康卡卡管系统与机构电子健康卡卡管系统同时上传数据到全国电子健康卡应用监测系统的情况，省级卡管在做数据上传时需过滤机构卡管数据。

3.2 数据采集交互流程



4 接口实现与调用

4.1 数据交互方式及数据格式

调用方式	HTTP
提交方式	POST
数据格式	提交和返回数据均为 JSON 格式
字符编码	统一采用 UTF-8 字符编码
判断逻辑	先判断协议字段返回，再判断业务返回，最后判断交易状态
签名算法	请求和响应均需要摘要验证，采用 SM3 算法

加密算法	请求和响应均需要加密通讯，采用 SM4 算法

5 卡管接口标准规范

5.1 管理查询类

序号	名称	描述	方法名
1	卡管节点网络查询	卡管节点基本信息	ehm.analysisdata.system.summary
2	接入机构基本信息查询	各个卡管接入的机构信息，以及接入时间等	ehm.analysisdata.org.summary
3	接入机构统计数据查询	统计医疗机构的建设受理情况数据	ehm.analysisdata.orgsum.statistics
4	客户端应用软件接入信息	各个卡管的客户端应用接入信息	ehm.analysisdata.clientsoftware.statistics
5	识读终端信息查询	各个卡管的识读终端接入信息	ehm.analysisdata.readterm.statistics
6	CA 证书验证	用于验证 ca 服务器证书	ehm.analysisdata.ca.cert

5.1.1 卡管节点网络查询

描述：卡管节点基本信息

数据采集频率：每天 02:00 采集

数据模式：全量

分页条件：根据 erhc_system_record_no 分页

请求参数

参数	参数名称	类型	可空	参数说明
公共请求参数				
method	接口名称	String(50)	N	ehm.analysisdata.system.summary
app_id	应用编号	String(32)	N	统一分配
term_id	终端编号	String(32)	N	统一分配
version	接口版本号	String(10)	N	X.M.0.1
timestamp	请求时间戳	String(20)	N	yyyyMMddHHmmss
digest_type	摘要类型	String(10)	N	SM3
digest	摘要内容	String(256)	Y	
enc_type	加密类型	String(10)	N	SM4
biz_content	请求参数集合	String(-)	N	无
<<接口请求参数>>				
page_no	查询页码	Number(5)	N	默认从 1 开始

page_size	每页数量	Number(5)	N	

响应参数

参数	参数名称	类型	可空	参数说明
公共响应参数				
ret_code	返回结果码	String(10)	N	
ret_msg	返回结果说明	String(200)	N	
app_id	应用编号	String(20)	N	与请求报文一致
method	接口名称	String(50)	N	与请求报文一致
version	接口版本号	String(10)	N	与请求报文一致
timestamp	响应报文时间戳	String(20)	N	
digest_type	摘要类型	String(10)	N	
digest	摘要内容	String(256)	N	
enc_type	加密类型	String(10)	Y	
biz_content	响应参数集合	String(-)	Y	响应参数的集合，最大长度不限，除公共响应参数外所有请求参数都必须放在这个参数中传递，具体参照各接口<<接口响应参数>>
<<接口响应参数>>				
system_info_list	卡管节点网络列表	JSONArray	N	格式详见 6.1.1
page_no	当前页码	Number(5)	N	
page_size	每页数量	Number(5)	N	
total_count	总数量	Number(10)	N	

5.1.2接入机构基本信息查询

描述：接入机构基本信息

数据采集频率：每天 02:00 采集

数据模式：全量

分页条件：根据 org_code 分页

请求参数

参数	参数名称	类型	可空	参数说明
公共请求参数				
method	接口名称	String(50)	N	ehm.analysisdata.org.summary
app_id	应用编号	String(32)	N	统一分配
term_id	终端编号	String(32)	N	统一分配

version	接口版本号	String(10)	N	X.M.0.1
timestamp	请求时间戳	String(20)	N	yyyyMMddHHmmss
digest_type	摘要类型	String(10)	N	SM3
digest	摘要内容	String(256)	Y	
enc_type	加密类型	String(10)	N	SM4
biz_content	请求参数集合	String(-)	N	无
<<接口请求参数>>				
page_no	查询页码	Number(5)	N	默认从 1 开始
page_size	每页数量	Number(5)	N	

响应参数

参数	参数名称	类型	可空	参数说明
公共响应参数				
ret_code	返回结果码	String(10)	N	
ret_msg	返回结果说明	String(200)	N	
app_id	应用编号	String(20)	N	与请求报文一致
method	接口名称	String(50)	N	与请求报文一致
version	接口版本号	String(10)	N	与请求报文一致
timestamp	响应报文时间戳	String(20)	N	
digest_type	摘要类型	String(10)	N	
digest	摘要内容	String(256)	N	
enc_type	加密类型	String(10)	Y	
biz_content	响应参数集合	String(-)	Y	响应参数的集合，最大长度不限，除公共响应参数外所有请求参数都必须放在这个参数中传递，具体参照各接口<<接口响应参数>>
<<接口响应参数>>				
org_list	接入机构列表	JSONArray	N	格式详见 6.1.2
page_no	当前页码	Number(5)	N	
page_size	每页数量	Number(5)	N	
total_count	总数量	Number(10)	N	

5.1.3接入机构统计数据查询

描述：接入机构统计信息，包含机构的终端数、接入日期、第一张发卡的时间、第一次用卡的时间等

数据采集频率：每天 02:00 采集

数据模式：全量

分页条件：根据 org_code 分页

请求参数

参数	参数名称	类型	可空	参数说明
公共请求参数				
method	接口名称	String(50)	N	ehm.analysisdata.orgsum.statistics
app_id	应用编号	String(32)	N	统一分配
term_id	终端编号	String(32)	N	统一分配
version	接口版本号	String(10)	N	X.M.0.1
timestamp	请求时间戳	String(20)	N	yyyyMMddHHmmss
digest_type	摘要类型	String(10)	N	SM3
digest	摘要内容	String(256)	Y	
enc_type	加密类型	String(10)	N	SM4
biz_content	请求参数集合	String(-)	N	无
<<接口请求参数>>				
page_no	查询页码	Number(5)	N	默认从 1 开始
page_size	每页数量	Number(5)	N	

响应参数

参数	参数名称	类型	可空	参数说明
公共响应参数				
ret_code	返回结果码	String(10)	N	
ret_msg	返回结果说明	String(200)	N	
app_id	应用编号	String(20)	N	与请求报文一致
method	接口名称	String(50)	N	与请求报文一致
version	接口版本号	String(10)	N	与请求报文一致
timestamp	响应报文时间戳	String(20)	N	
digest_type	摘要类型	String(10)	N	
digest	摘要内容	String(256)	N	
enc_type	加密类型	String(10)	Y	
biz_content	响应参数集合	String(-)	Y	响应参数的集合，最大长度不限，除公共响应参数外所有请求参数都必须放在这个参数中传递，具体参照各接口<<接口响应参数>>
<<接口响应参数>>				
org_sum_list	接入机构统计列表	JSONArray	N	格式详见 6.1.3
page_no	当前页码	Number(5)	N	
page_size	每页数量	Number(5)	N	
total_count	总数量	Number(10)	N	

5.1.4客户端应用软件接入信息查询

描述：备案的客户端信息
数据采集频率：每天 02:00 采集
数据模式：全量
分页条件：根据 org_code 分页

请求参数

参数	参数名称	类型	可空	参数说明
公共请求参数				
method	接口名称	String(50)	N	ehm.analysisdata.clientsoftware.statistics
app_id	应用编号	String(32)	N	统一分配
term_id	终端编号	String(32)	N	统一分配
version	接口版本号	String(10)	N	X.M.0.1
timestamp	请求时间戳	String(20)	N	yyyyMMddHHmmss
digest_type	摘要类型	String(10)	N	SM3
digest	摘要内容	String(256)	Y	
enc_type	加密类型	String(10)	N	SM4
biz_content	请求参数集合	String(-)	N	请求参数的集合，最大长度不限，除公共请求参数外所有请求参数都必须放在这个参数中传递，具体参照各接口<<接口请求参数>>
<<接口请求参数>>				
page_no	查询页码	Number(5)	N	默认从 1 开始
page_size	每页数量	Number(5)	N	

响应参数

参数	参数名称	类型	可空	参数说明
公共响应参数				
ret_code	返回结果码	String(10)	N	
ret_msg	返回结果说明	String(200)	N	
app_id	应用编号	String(20)	N	与请求报文一致
method	接口名称	String(50)	N	与请求报文一致
version	接口版本号	String(10)	N	与请求报文一致
timestamp	响应报文时间戳	String(20)	N	
digest_type	摘要类型	String(10)	N	
digest	摘要内容	String(256)	N	
enc_type	加密类型	String(10)	Y	
biz_content	响应参数集合	String(-)	Y	响应参数的集合，最大长度不限，除公共响应参数外所有请求参数都必须放在这个参数中传递，

				具体参照各接口<<接口响应参数>>
<<接口响应参数>>				
client_software_list	客户端应用软件统计列表	JSONArray	N	格式详见 6.1.5
page_no	当前页码	Number(5)	N	
page_size	每页数量	Number(5)	N	
total_count	总数量	Number(10)	N	

5.1.5 识读终端信息查询

描述：备案的识读终端信息
数据采集频率：每天 02:00 采集
数据模式：全量
分页条件：根据 org_code 分页

请求参数

参数	参数名称	类型	可空	参数说明
公共请求参数				
method	接口名称	String(50)	N	ehm.analysisdata.readterm.statistics
app_id	应用编号	String(32)	N	统一分配
term_id	终端编号	String(32)	N	统一分配
version	接口版本号	String(10)	N	X.M.0.1
timestamp	请求时间戳	String(20)	N	yyyyMMddHHmmss
digest_type	摘要类型	String(10)	N	SM3
digest	摘要内容	String(256)	Y	
enc_type	加密类型	String(10)	N	SM4
biz_content	请求参数集合	String(-)	N	请求参数的集合，最大长度不限，除公共请求参数外所有请求参数都必须放在这个参数中传递，具体参照各接口<<接口请求参数>>
<<接口请求参数>>				
page_no	查询页码	Number(5)	N	默认从 1 开始
page_size	每页数量	Number(5)	N	

响应参数

参数	参数名称	类型	可空	参数说明
公共响应参数				
ret_code	返回结果码	String(10)	N	
ret_msg	返回结果说明	String(200)	N	
app_id	应用编号	String(20)	N	与请求报文一致
method	接口名称	String(50)	N	与请求报文一致
version	接口版本号	String(10)	N	与请求报文一致
timestamp	响应报文时间戳	String(20)	N	

digest_type	摘要类型	String(10)	N	
digest	摘要内容	String(256)	N	
enc_type	加密类型	String(10)	Y	
biz_content	响应参数集合	String(-)	Y	响应参数的集合，最大长度不限，除公共响应参数外所有请求参数都必须放在这个参数中传递，具体参照各接口<<接口响应参数>>
<<接口响应参数>>				
read_term_list	识读终端统计列表	JSONArray	N	格式详见 6.1.4
page_no	当前页码	Number(5)	N	
page_size	每页数量	Number(5)	N	
total_count	总数量	Number(10)	N	

5.1.6CA 证书验证

描述：用于验证 ca 服务器证书,当证书验证通过后,采集其他接口数据
数据采集频率：每天 02:00 采集
数据模式：全量

请求参数

参数	参数名称	类型	可空	参数说明
公共请求参数				
method	接口名称	String(50)	N	ehm.analysisdata.ca.cert
app_id	应用编号	String(32)	N	统一分配
term_id	终端编号	String(32)	N	统一分配
version	接口版本号	String(10)	N	X.M.0.1
timestamp	请求时间戳	String(20)	N	yyyyMMddHHmmss
digest_type	摘要类型	String(10)	N	SM3
digest	摘要内容	String(256)	Y	
enc_type	加密类型	String(10)	N	SM4
biz_content	请求参数集合	String(-)	N	请求参数的集合，最大长度不限，除公共请求参数外所有请求参数都必须放在这个参数中传递，具体参照各接口<<接口请求参数>>
<<接口请求参数>>				
page_no	查询页码	Number(5)	N	默认从 1 开始
page_size	每页数量	Number(5)	N	

响应参数

参数	参数名称	类型	可空	参数说明
公共响应参数				
ret_code	返回结果码	String(10)	N	
ret_msg	返回结果说明	String(200)	N	
app_id	应用编号	String(20)	N	与请求报文一致

method	接口名称	String(50)	N	与请求报文一致
version	接口版本号	String(10)	N	与请求报文一致
timestamp	响应报文时间戳	String(20)	N	
digest_type	摘要类型	String(10)	N	
digest	摘要内容	String(256)	N	
enc_type	加密类型	String(10)	Y	
biz_content	响应参数集合	String(-)	Y	响应参数的集合，最大长度不限，除公共响应参数外所有请求参数都必须放在这个参数中传递，具体参照各接口<<接口响应参数>>
<<接口响应参数>>				
cert_list	ca 服务器证书列表	JSONArray	N	格式详见 6.1.6
page_no	当前页码	Number(5)	N	
page_size	每页数量	Number(5)	N	
total_count	总数量	Number(10)	N	

5.2 实时监测类

序号	名称	描述	方法名
1	发卡用卡数据查询	每天每个机构每个性别每个渠道，发卡总数，用卡次总数	ehm.analysisdata.ehcsum.statistics
2	用卡诊疗环节数据查询	每天每个机构线上线下每个诊疗环节的用卡次数	ehm.analysisdata.usescene.statistics
3	累计支付数据查询	每天每个机构每个支付渠道支付笔数与支付金额	ehm.analysisdata.paysum.statistics
4	出生年份发卡用卡支付数据	每天每个机构每个出生年份发卡总数用卡总数支付总数	ehm.analysisdata.ehcbirth.statistics
5	发卡证件数据查询	每天每个机构每种证件发卡总数	ehm.analysisdata.certificates.statistics

5.2.1 发卡用卡数据查询

描述：时间段内按照机构、性别、渠道统计发卡数、用卡数

数据采集频率：每天 03:00 采集上一天

数据模式：增量

分页条件：根据 org_code 分页

请求参数

参数	参数名称	类型	可空	参数说明
公共请求参数				

method	接口名称	String(50)	N	ehm.analysisdata.ehcsum.statistics
app_id	应用编号	String(32)	N	统一分配
term_id	终端编号	String(32)	N	统一分配
version	接口版本号	String(10)	N	X.M.0.1
timestamp	请求时间戳	String(20)	N	yyyyMMddHHmmss
digest_type	摘要类型	String(10)	N	SM3
digest	摘要内容	String(256)	Y	
enc_type	加密类型	String(10)	N	SM4
biz_content	请求参数集合	String(-)	N	请求参数的集合，最大长度不限，除公共请求参数外所有请求参数都必须放在这个参数中传递，具体参照各接口<<接口请求参数>>
<<接口请求参数>>				
collect_time	采集数据日期	String(8)	N	yyyyMMdd（查询日期 00:00:00 到下一天 00:00:00 的数据）
page_no	查询页码	Number(5)	N	默认从 1 开始
page_size	每页数量	Number(5)	N	

响应参数

参数	参数名称	类型	可空	参数说明
公共响应参数				
ret_code	返回结果码	String(10)	N	
ret_msg	返回结果说明	String(200)	N	
app_id	应用编号	String(20)	N	与请求报文一致
method	接口名称	String(50)	N	与请求报文一致
version	接口版本号	String(10)	N	与请求报文一致
timestamp	响应报文时间戳	String(20)	N	
digest_type	摘要类型	String(10)	N	
digest	摘要内容	String(256)	N	
enc_type	加密类型	String(10)	Y	
biz_content	响应参数集合	String(-)	Y	响应参数的集合，最大长度不限，除公共响应参数外所有请求参数都必须放在这个参数中传递，具体参照各接口<<接口响应参数>>
<<接口响应参数>>				
ehc_sum_ list	累计发卡用卡统计列表	JSONArray	N	格式详见 6.2.1
page_no	当前页码	Number(5)	N	
page_size	每页数量	Number(5)	N	
total_count	总数量	Number(10)	N	

5.2.2用卡诊疗环节数据查询

描述：时间段内按照机构、诊疗环节统计用卡数

数据采集频率：每天 03:00 采集上一天

数据模式：增量

分页条件：根据 org_code 分页

请求参数

参数	参数名称	类型	可空	参数说明
公共请求参数				
method	接口名称	String(50)	N	ehm.analysisdata.usescene.statistics
app_id	应用编号	String(32)	N	统一分配
term_id	终端编号	String(32)	N	统一分配
version	接口版本号	String(10)	N	X.M.0.1
timestamp	请求时间戳	String(20)	N	yyyyMMddHHmmss
digest_type	摘要类型	String(10)	N	SM3
digest	摘要内容	String(256)	Y	
enc_type	加密类型	String(10)	N	SM4
biz_content	请求参数集合	String(-)	N	请求参数的集合，最大长度不限，除公共请求参数外所有请求参数都必须放在这个参数中传递，具体参照各接口<<接口请求参数>>
<<接口请求参数>>				
collect_time	采集数据日期	String(8)	N	yyyyMMdd（查询日期 00:00:00 到下一天 00:00:00 的数据）
page_no	查询页码	Number(5)	N	默认从 1 开始
page_size	每页数量	Number(5)	N	

响应参数

参数	参数名称	类型	可空	参数说明
公共响应参数				
ret_code	返回结果码	String(10)	N	
ret_msg	返回结果说明	String(200)	N	
app_id	应用编号	String(20)	N	与请求报文一致
method	接口名称	String(50)	N	与请求报文一致
version	接口版本号	String(10)	N	与请求报文一致
timestamp	响应报文时间戳	String(20)	N	
digest_type	摘要类型	String(10)	N	
digest	摘要内容	String(256)	N	
enc_type	加密类型	String(10)	Y	
biz_content	响应参数集合	String(-)	Y	响应参数的集合，最大长度不限，除公共响应参数外所有请求参数都必须放在这个参数中传递，具体参照各接口<<接口响应参数>>

<<接口响应参数>>				
usecard_scene_list	用卡环节统计列表	JSONArray	N	格式详见 6.2.2
page_no	当前页码	Number(5)	N	
page_size	每页数量	Number(5)	N	
total_count	总数量	Number(10)	N	

5.2.3累计支付数据查询

描述：时间段内按照机构、支付渠道统计支付次数、支付金额

数据采集频率：每天 03:00 采集上一天

数据模式：增量

分页条件：根据 org_code 分页

请求参数

参数	参数名称	类型	可空	参数说明
公共请求参数				
method	接口名称	String(50)	N	ehm.analysisdata.paysum.statistics
app_id	应用编号	String(32)	N	统一分配
term_id	终端编号	String(32)	N	统一分配
version	接口版本号	String(10)	N	X.M.0.1
timestamp	请求时间戳	String(20)	N	yyyyMMddHHmmss
digest_type	摘要类型	String(10)	N	SM3
digest	摘要内容	String(256)	Y	
enc_type	加密类型	String(10)	N	SM4
biz_content	请求参数集合	String(-)	N	请求参数的集合，最大长度不限，除公共请求参数外所有请求参数都必须放在这个参数中传递，具体参照各接口<<接口请求参数>>
<<接口请求参数>>				
collect_time	采集数据日期	String(8)	N	yyyyMMdd（查询日期 00:00:00 到下一天 00:00:00 的数据）
page_no	查询页码	Number(5)	N	默认从 1 开始
page_size	每页数量	Number(5)	N	

响应参数

参数	参数名称	类型	可空	参数说明
公共响应参数				
ret_code	返回结果码	String(10)	N	

ret_msg	返回结果说明	String(200)	N	
app_id	应用编号	String(20)	N	与请求报文一致
method	接口名称	String(50)	N	与请求报文一致
version	接口版本号	String(10)	N	与请求报文一致
timestamp	响应报文时间戳	String(20)	N	
digest_type	摘要类型	String(10)	N	
digest	摘要内容	String(256)	N	
enc_type	加密类型	String(10)	Y	
biz_content	响应参数集合	String(-)	Y	响应参数的集合，最大长度不限，除公共响应参数外所有请求参数都必须放在这个参数中传递，具体参照各接口<<接口响应参数>>
<<接口响应参数>>				
pay_sum_list	累计支付统计列表	JSONArray	N	格式详见 6.2.3
page_no	当前页码	Number(5)	N	
page_size	每页数量	Number(5)	N	
total_count	总数量	Number(10)	N	

5.2.4发卡用卡支付数据查询

描述：时间段内按照机构、出生日期统计发卡数、用卡数、支付笔数

数据采集频率：每天 03:00 采集上一天

数据模式：增量

分页条件：根据 org_code、birth_year 分页

请求参数

参数	参数名称	类型	可空	参数说明
公共请求参数				
method	接口名称	String(50)	N	ehm.analysisdata.ehcbirth.statistics
app_id	应用编号	String(32)	N	统一分配
term_id	终端编号	String(32)	N	统一分配
version	接口版本号	String(10)	N	X.M.0.1
timestamp	请求时间戳	String(20)	N	yyyyMMddHHmmss
digest_type	摘要类型	String(10)	N	SM3
digest	摘要内容	String(256)	Y	
enc_type	加密类型	String(10)	N	SM4
biz_content	请求参数集合	String(-)	N	请求参数的集合，最大长度不限，除公共请求参数外所有请求参数都必须放在这个参数中传递，具体参照各接口<<接口请求参数>>
<<接口请求参数>>				

collect_time	采集数据日期	String(8)	N	yyyyMMdd（查询日期 00:00:00 到下一天 00:00:00 的数据）
page_no	查询页码	Number(5)	N	默认从 1 开始
page_size	每页数量	Number(5)	N	

响应参数

参数	参数名称	类型	可空	参数说明
公共响应参数				
ret_code	返回结果码	String(10)	N	
ret_msg	返回结果说明	String(200)	N	
app_id	应用编号	String(20)	N	与请求报文一致
method	接口名称	String(50)	N	与请求报文一致
version	接口版本号	String(10)	N	与请求报文一致
timestamp	响应报文时间戳	String(20)	N	
digest_type	摘要类型	String(10)	N	
digest	摘要内容	String(256)	N	
enc_type	加密类型	String(10)	Y	
biz_content	响应参数集合	String(-)	Y	响应参数的集合，最大长度不限，除公共响应参数外所有请求参数都必须放在这个参数中传递，具体参照各接口<<接口响应参数>>
<<接口响应参数>>				
ehc_birth_list	各出生年份发卡数列表	JSONArray	N	格式详见 6.2.4
page_no	当前页码	Number(5)	N	
page_size	每页数量	Number(5)	N	
total_count	总数量	Number(10)	N	

5.2.5发卡证件数据查询

描述：时间段内按照机构、证件类型统计发卡数

数据采集频率：每天 03:00 采集上一天

数据模式：增量

分页条件：根据 org_code 分页

请求参数

参数	参数名称	类型	可空	参数说明
公共请求参数				
method	接口名称	String(50)	N	ehm.analysisdata.certificates.statistics
app_id	应用编号	String(32)	N	统一分配

term_id	终端编号	String(32)	N	统一分配
version	接口版本号	String(10)	N	X.M.0.1
timestamp	请求时间戳	String(20)	N	yyyyMMddHHmmss
digest_type	摘要类型	String(10)	N	SM3
digest	摘要内容	String(256)	Y	
enc_type	加密类型	String(10)	N	SM4
biz_content	请求参数集合	String(-)	N	请求参数的集合，最大长度不限，除公共请求参数外所有请求参数都必须放在这个参数中传递，具体参照各接口<<接口请求参数>>
<<接口请求参数>>				
collect_time	采集数据日期	String(8)	N	yyyyMMdd（查询日期 00:00:00 到下一天 00:00:00 的数据）
page_no	查询页码	Number(5)	N	默认从 1 开始
page_size	每页数量	Number(5)	N	

响应参数

参数	参数名称	类型	可空	参数说明
公共响应参数				
ret_code	返回结果码	String(10)	N	
ret_msg	返回结果说明	String(200)	N	
app_id	应用编号	String(20)	N	与请求报文一致
method	接口名称	String(50)	N	与请求报文一致
version	接口版本号	String(10)	N	与请求报文一致
timestamp	响应报文时间戳	String(20)	N	
digest_type	摘要类型	String(10)	N	
digest	摘要内容	String(256)	N	
enc_type	加密类型	String(10)	Y	
biz_content	响应参数集合	String(-)	Y	响应参数的集合，最大长度不限，除公共响应参数外所有请求参数都必须放在这个参数中传递，具体参照各接口<<接口响应参数>>
<<接口响应参数>>				
certificates_opencard_list	发卡证件分析列表	JSONArray	N	格式详见 6.2.5
page_no	当前页码	Number(5)	N	
page_size	每页数量	Number(5)	N	
total_count	总数量	Number(10)	N	

6 卡管接口标准规范

6.1 管理查询类

6.1.1 system_info_list 卡管节点网络列表

<< list 定义>>					
参数	**参数名称**	**类型**	**可空**	**参数说明**	**示例**
erhc_system_record_no	卡管节点入网编码(EHCIN)	String(50)	N	卡管节点入网编码	
erhc_system	卡管节点名称	String(50)	N	卡管节点名称	电子健康卡 XXX 管理节点
city_code	所属城市行政区划代码	String(32)	N	地级市城市编码	350200
org_code	组织机构代码	String(32)	N	医疗机构根据《WS 218 卫生机构（组织）代码》填写医疗机构执业许可证登记号；卫生管理机构等填写统一社会信用代码	例如：医疗机构执业许可证登记号（22 位）：73843029333030217A3591; 统一社会信用代码（18 位）：11320982K13082661K
org_name	机构名称	String(50)	N	医疗卫生机构名称	
system_level	节点级别	Number(5)	N	节点级别，根据卡管节点层级关系，如顶节点为 1 级，次节点为 2 级，依次类推	国家为 1 级,直连国家为 2 级,非直连国家,由 2 级卡管代为上传的节点为 3 级 例如:直连国家的卡管节点,此字段级别为:2
owner	建设单位名称	String(50)	N	建设单位名称	省、市的管理节点承建单位，例如：XXX 卫健委、XXX 医院、XXX 公共卫生机构等；
online_time	上线日期	String(8)	N	上线日期	yyyyMMdd
parent_system	上级节点名称	String(50)	Y	上级卡管节点名称	
parent_system_record_no	上级管理节点入网编码（EHCIN）	String(50)	Y	上级卡管节点入网编码	3 级节点上级为本省 2 级节点的入网编码，2 级节点上级为 00000000；
deployment_location	部署物理地址	String(200)	N	物理部署地址,如:上海政务机房,多地址用英文	

				逗号分隔	
system_url	节点入网地址	String(100)	N	节点入网地址	填写节点政务网IP
mgr_system_name	管理系统名称	String(50)	N	电子健康卡管理系统产品名称	
copyright_no	著作权编号	String(50)	Y	计算器软件著作权登记号	2021SR***035
manufacturer	生产单位	String(50)	N	开发商名称	
follow_version	遵循标准版本号	String(50)	N	遵循《电子健康卡建设与管理指南（试行）》标准版本号	例如：2.4、3.0
test_certificate	标准符合性证明	Number(5)	N	0 未检测 1 已检测 说明：仅已完成检测为 1 其余为 0	
test_date	检测日期	String(8)	Y	检测通过时间	
encryption_equipment_list	加密机列表	JSONArray	N	加密机信息列表	
<< encryption_equipment_list 定义>>					
参数	**参数名称**	**类型**	**可空**	**参数说明**	**示例**
product_name	产品序列号	String(50)	N		
product_model	加密机型号	String(50)	N		
manufacturer	加密机生产厂商	String(50)	N	加密机生产厂商名称	
dealer	加密机销售厂商	String(50)	N	加密机销售厂商名称	

6.1.2 org_list 接入机构基本信息

<<list 定义>>					
参数	**参数名称**	**类型**	**可空**	**参数说明**	**示例**
province_code	所属省份行政区划代码	String(32)	N	6 位行政编码，	350000
city_code	所属城市行政区划代码	String(32)	N	地级市城市编码	350200
org_code	组织机构代码	String(32)	N	医疗机构根据《WS 218 卫生机构（组织）代码》填写医疗机构执业许可证登记号；卫生管理机构等填写统一社会信用代码	例如：医疗机构执业许可证登记号（22 位）：73843029333030217A3591; 统一社会信用代码（18 位）：11320982K13082661K
org_name	机构名称	String(50)	N	医疗卫生机构名称	
org_level	机构等级	String(32)	N	见 7.3 医疗机构等级编码表	
org_type	机构类别	String(32)	N	见 7.4 医疗机构类别编	

				码表	
org_property	机构性质	String(32)	N	1：公立 2：民办 99:其他	
erhc_system_record_no	所属卡管节点入网编码(EHCIN)	String(50)	N	所属卡管节点入网编码	

示例数据与格式

```
[
    {
        "province_code ": "350000",
        "city_code": "350200",
        "org_code": "426600687",
        "org_name": "厦门某医院",
        "org_level": "031",
        "org_property": "01",
        "org_type": "01"
    },
    {
        "province_code ": "350000",
        "city_code": "350100",
        "org_code": "426600688",
        "org_name": "福州某医院",
        "org_level": "031",
        "org_property": "01",
        "org_type": "01"
    }
]
```

6.1.3 org_sum_list 接入机构统计列表

<< list 定义>>					
参数	**参数名称**	**类型**	**可空**	**参数说明**	**示例**
org_code	组织机构代码	String(32)	N	医疗机构根据《WS 218 卫生机构（组织）代码》填写医疗机构执业许可证登记号;卫生管理机构等填写统一社会信用代码	例如:医疗机构执业许可证登记号（22 位）：73843029333030217A3591; 统一社会信用代码（18 位）：11320982K13082661K
org_access_time	接入机构日期	String(8)	Y	yyyyMMdd	

org_access_address	接入机构系统地址	String(50)	Y	机构接入的信息系统 的 IP 地址	
first_reg_time	第一张发卡的时间(完成灌密后)	String(32)	Y	yyyyMMddHHmmss	
first_usecard_time	第一次用卡的时间	String(14)	Y	yyyyMMddHHmmss	
accept_status	是否可受理健康卡	String(5)	N	0-可以,1-不可以	
accept_time	开始受理健康卡日期	String(8)	Y	yyyyMMdd 用户第一次生成二维码的日期	
win_term_num	接入机构窗口部署终端数	Number(24)	Y	无数据请填写“0”	
sst_term_num	接入机构自助机部署终端数	Number(24)	Y	无数据请填写“0”	
other_term_num	接入机构其他部署终端数	Number(24)	Y	无数据请填写“0”	

6.1.4 read_term_list 识读终端统计列表

<< list 定义>>					
参数	**参数名称**	**类型**	**可空**	**参数说明**	**示例**
org_code	组织机构代码	String(32)	N	医疗机构根据《WS 218 卫生机构（组织）代码》填写医疗机构执业许可证登记号；卫生管理机构等填写统一社会信用代码	例如:医疗机构执业许可证登记号（ 22 位 ）：73843029333030217A3591; 统一社会信用代码（ 18 位）：11320982K13082661K
org_name	机构名称	String(32)	N		
term_record	终端接入号	String(50)	N	由电子健康卡管理信息系统分配	
term_serial	终端出厂序列号	String(50)	N	通常为数字或字母形 式	
term_name	终端名称	String(50)	N	终端内部名称	挂号自助终端
term_useway	终端用途	String(50)	N	描述终端用途	用于患者自助进行挂号等操作
term_unit	终端开发单位	String(50)	N	工商注册名称	
term_access_time	终端接入日期	String(8)	N	yyyyMMdd	

6.1.5 client_software_list 客户端应用软件统计列表

<< list 定义>>					
参数	**参数名称**	**类型**	**可空**	**参数说明**	**示例**
org_code	组织机构代码	String(32)	N	医疗机构根据《WS 218 卫生机构	例如：医疗机构执业许可证

<< list 定义>>					
参数	**参数名称**	**类型**	**可空**	**参数说明**	**示例**
				（组织）代码》填写医疗机构执业许可证登记号；卫生管理机构等填写统一社会信用代码	登记号（22位）：73843029333030217A3591; 统一社会信用代码（18位）：11320982K13082661K
record_num	登记编号(EHCAPPID)	String(32)	N	由电子健康卡管理信息系统分配，编号规则见附录D.2； APP Android、APP iOS、公众号、服务号等每个应用种类均应分配唯一编号；	例如：1101A0056APPA0001
app_name	应用名称	String(50)	N	客户端应用软件显示给用户的名称	
app_channel	应用种类	String(50)	N	该项为选择项，不可任意填写文本种类列表见7.7应用种类一编码表	
app_version	应用版本号	String(50)	N	版本号 X.Y 形式，应至少包含大版本和小版本 2 级	例如：1.2 或者 1.2.1
app_category	应用服务种类（可多选）	String(50)	N	该项为多选项，不可任意填写文本， 种类列表见 7.8 应用种类二编码表（为空返回空，不能返回null。多个以英文逗号隔开）；	
app_package	应用包名	String(50)	Y	仅 APP 填写，app应用包名	例如： com.ehealth.hospital
dev_unit	开发单位名称	String(50)	N	工商注册名称	填写全称
use_unit	应用运营机构名称	String(50)	N	应用的运营责任承担主体	
use_unit_type	运营机构类型	String(10)	N	A 卫健委；B 医院；C 公共卫生机构；D 基层卫生机构；E 政府其他部门；F 第三方机构；X 其他	A
use_unit_people	运营机构联系人	String(50)	N		
use_unit_phone	运营机构联系方式	String(50)	N		
use_unit_mail	运营机构邮箱	String(50)	N		
copyright_no	应用著作权编号	String(50)	Y	应用的著作权登记号	2021SR***035
icp_no	应用ICP备案编号	String(50)	Y	应用的ICP备案编号	
djbh_no	应用等保报告编号	String(50)	Y	应用取得的等保报告编号	
record_time	应用接入日期	String(8)	N	接入电子健康卡系统时间，分配接入编号的日期，格式：年月日	例如：20201001

<< list 定义>>					
参数	**参数名称**	**类型**	**可空**	**参数说明**	**示例**
				yyyyMMdd	
launch_time	应用上线日期	String(8)	Y	应用正式上线日期，格式：年月日 yyyyMMdd	例如：20201001
app_url	应用地址	String(100)	N	APP 填写下载地址 公众号、小程序等填写域名地址	例如：https://itunes.apple.com/cn/app/id1398635899?mt=8
img_url	应用 logo 地址	String(100)	N	公众号、小程序、APP 的可以进行引用的 logo 地址，	例如：https:// 应用域名/icon.png
release_channel	发布渠道	String(50)	Y	仅 APP 填写；该项为选择项，不可任意填写文本，渠道列表详见附录 B 发布渠道编码表（为空返回空，不能返回 null。多个以英文逗号隔开）	
erhc_system	接入的卡管节点名称	String(50)	N	由电子健康卡管理系统自动关联填写	如北京西城管理节点
erhc_system_record_no	卡管节点入网编码(EHCIN)	String(50)	N	由电子健康卡管理系统自动关联填写	1101A0056
online_status	应用在线状态	String(5)	N	由电子健康卡管理系统判断应用在线联通状态 1-联网 2-未联网 3-停用	1

6.1.6 cert_list ca 服务器证书列表

<< list 定义>>					
参数	**参数名称**	**类型**	**可空**	**参数说明**	**示例**
cert	服务器证书	String	N	ca 服务器证书,base64 格式	

6.2 实时监测类

6.2.1 ehc_sum_list 发卡用卡统计列表

<< list 定义>>					
参数	**参数名称**	**类型**	**可空**	**参数说明**	**示例**
time_region	统计日期时间	String(20)	N	yyyyMMdd	
org_code	组织机构代码	String(32)	N	医疗机构根据《WS 218 卫生机构（组织）代码》填写医疗机构执业许可证登记号；卫生管理机构等填写统一社会信用代	例如:医疗机构执业许可证登记号（22 位）：73843029333030217A3591;

				码	统一社会信用代码（18 位）：11320982K13082661K
regcard_sex	性别编码	String(32)	N	7.2 性别编码表	
regcard_channel	渠道编码	String(32)	N	7.7 应用种类一编码表	
regcard _num	发卡数（包含预制卡）	Number(24)	N	发卡数=开卡数+预制卡总数，无数据请填写“0”	
activate_num	激活数（用户主动申领电子健康卡）	Number(24)	N	用户有申领操作就算一次，一个用户只统计一次。无数据请填写“0”	
usecard _num	用卡数	Number(24)	N	一个用户可以有多次用卡数,无数据请填写“0”	
usecard _people_num	用卡人次	Number(24)	N	一个用户只能算一次,无数据请填写“0”	

6.2.2 usecard_scene_list 用卡诊疗环节统计列表

<< list 定义>>					
参数	**参数名称**	**类型**	**可空**	**参数说明**	**示例**
time_region	统计日期时间	String(20)	N	yyyyMMdd	
org_code	组织机构代码	String(32)	N	医疗机构根据《WS 218 卫生机构（组织）代码》填写医疗机构执业许可证登记号;卫生管理机构等填写统一社会信用代码	例如:医疗机构执业许可证登记号（22 位）：73843029333030217A3591; 统一社会信用代码（18 位）：11320982K13082661K
online_or_offline	线上还是线下	String(20)	N	online:线上 offline:线下	
usecard_scene	用卡环节类型	String(32)	N	7.5 诊疗环节编码表	
usecard_scene_num	用卡数	Number(24)	N	无数据请填写“0”	

6.2.3 pay_sum_list 累计支付统计列表

<< list 定义>>					
参数	**参数名称**	**类型**	**可空**	**参数说明**	**示例**
time_region	统计日期时间	String(20)	N	yyyyMMdd	
org_code	组织机构代码	String(32)	N	医疗机构根据《WS 218	例如:医疗机构执

				卫生机构（组织）代码》填写医疗机构执业许可证登记号；卫生管理机构等填写统一社会信用代码	业许可证登记号（22 位）：73843029333030217A3591; 统一社会信用代码（18 位）：11320982K13082661K
pay_channel	支付渠道	String(32)	N	7.6 支付渠道编码表	
pay_num	支付笔数	Number(24)	N	无数据请填写“0”	
pay_amt	支付金额	Number(24,2)	N	无数据请填写“0”	

6.2.4 ehc_birth_list 出生年份发卡用卡支付统计列表

<< list 定义>>					
参数	**参数名称**	**类型**	**可空**	**参数说明**	**示例**
time_region	统计日期时间	String(20)	N	yyyyMMdd	
org_code	组织机构代码	String(32)	N	医疗机构根据《WS 218 卫生机构（组织）代码》填写医疗机构执业许可证登记号；卫生管理机构等填写统一社会信用代码	例如：医疗机构执业许可证登记号（22 位）：73843029333030217A3591; 统一社会信用代码（18 位）：11320982K13082661K
birth_year	出生年份	String(4)	N	yyyy	1990
regcard _num	发卡数	Number(24)	N	无数据请填写“0”	
usecard_num	用卡数	Number(24)	N	无数据请填写“0”	
pay_num	支付笔数	Number(24)	N	无数据请填写“0”	

6.2.5 certificates_opencard_list 发卡证件统计列表

<< list 定义>>					
参数	**参数名称**	**类型**	**可空**	**参数说明**	**示例**
time_region	统计日期时间	String(20)	N	yyyyMMdd	
org_code	组织机构代码	String(32)	N	医疗机构根据《WS 218 卫生机构（组织）代码》填写医疗机构执业许可证登记号；卫生管理机构等填写统一社会信用代码	例如：医疗机构执业许可证登记号（22 位）：73843029333030217A3591; 统一社会信用代码（18 位）：

					11320982K13082661K
id_type	证件类型	String(32)	N	7.1 证件类型编码表	
certificates_num	数量	Number(24)	N	无数据请填写“0”	

7 字典定义

7.1 证件类型编码表

证件代码	证件说明
01	居民身份证
02	居民户口簿
03	护照
04	军官证
05	驾驶证
06	港澳居民来往内地通行证
07	台湾居民来往内地通行证
08	出生医学证明
99	其他法定有效证件

7.2 性别编码表

名称	编码	说明
未知性别	0	
男	1	
女	2	
女性改（变）为男性	5	
男性改（变）为女性	6	
未说明性别	9	

7.3 医疗机构等级编码表

等级代码	等级名称	说明
030	三级	
032	三级甲等	
033	三级乙等	
034	三级丙等	
039	三级未评	
020	二级	
022	二级甲等	
023	二级乙等	
024	二级丙等	
029	二级未评	
010	一级	
012	一级甲等	
013	一级乙等	
014	一级丙等	
019	一级未评	

099	其他（非医疗机构或不属于以上等级的医疗机构）	

7.4 医疗机构类别编码表

代码	名称	说明
A	**医院**	
A100	综合医院	
A2	中医医院	
A210	中医(综合)医院	
A220	中医专科医院	
A221	肛肠医院	
A222	骨伤医院	包括正骨医院
A223	针灸医院	
A224	按摩医院	
A229	其他中医专科医院	
A300	中西医结合医院	
A4	民族医院	
A411	蒙医院	
A412	藏医院	
A413	维医院	
A414	傣医院	
A419	其他民族医院	
A5	专科医院	不含中医专科医院
A511	口腔医院	包括牙科医院
A512	眼科医院	
A513	耳鼻喉科医院	包括五官科医院
A514	肿瘤医院	
A515	心血管病医院	
A516	胸科医院	
A517	血液病医院	
A518	妇产(科)医院	包括妇婴(儿)医院
A519	儿童医院	
A520	精神病医院	包括 20 张床位以上的精神卫生中心
A521	传染病医院	
A522	皮肤病医院	包括性病医院
A523	结核病医院	
A524	麻风病医院	

A525	职业病医院	
A526	骨科医院	
A527	康复医院	
A528	整形外科医院	包括整容医院
A529	美容医院	
A539	其他专科医院	
A600	疗养院	不包括休养所
A7	护理院(站)	
A710	护理院	
A720	护理站	
B	**社区卫生服务中心（站）**	
B100	社区卫生服务中心	
B200	社区卫生服务站	
C	**卫生院**	
C100	街道卫生院	
C2	乡镇卫生院	
C210	中心卫生院	
C220	乡卫生院	
D	**门诊部、诊所、医务室、村卫生室**	包括卫生所(室)
D1	门诊部	
D110	综合门诊部	
D120	中医门诊部	
D121	中医(综合)门诊部	
D122	中医专科门诊部	
D130	中西医结合门诊部	
D140	民族医门诊部	
D150	专科门诊部	不含中医专科门诊部
D151	普通专科门诊部	
D152	口腔门诊部	
D153	眼科门诊部	
D154	医疗美容门诊部	
D155	精神卫生门诊部	
D159	其他专科门诊部	
D2	诊所	
D211	普通诊所	
D212	中医诊所	

D213	中西医结合诊所	
D214	民族医诊所	
D215	口腔诊所	
D216	医疗美容诊所	
D217	精神卫生诊所	
D229	其他诊所	
D300	卫生所(室)	
D400	医务室	
D500	中小学卫生保健所	
D600	村卫生室	
E	**急救中心（站）**	
E100	急救中心	
E200	急救中心站	
E300	急救站	
F	**采供血机构**	
F1	血站	
F110	血液中心	
F120	中心血站	
F130	基层血站、中心血库	
F200	单采血浆站	
G	**妇幼保健院(所、站)**	包括妇幼保健中心
G100	妇幼保健院	
Z	**其他**	
Z100	卫健委	
Z999	其他类别	

7.5 诊疗环节编码表

父用卡环节代码	父环节名称	子用卡环节代码	子环节名称	用卡环节代码	用卡环节名称
01010	门诊、住院服务	010101	预约挂号	0101011	预约挂号
				0101012	当日挂号
				0101013	挂号记录
				0101014	预约导诊
				0101015	住院预约
				0101016	医技预约
				0101017	体检预约
				0101018	婚检预约
				0101019	孕检孕检

		010102	诊断	0101021	排队候诊
				0101022	门诊记录
				0101023	病历打印
				0101024	就医反馈
		010103	取药		
		010104	检验检查		
		010105	收费	0101051	门诊缴费
				0101052	门诊缴费记录
				0101053	住院缴费
				0101054	住院缴费记录
				0101055	门诊充值
				0101056	住院充值
				0101057	挂号退费
		010106	开方		
		010107	手术		
		010108	病案调阅（电子病历）		
		010109	报告单查询		
		010110	智能导诊		
		010111	排队叫号		
		010112	候诊提醒		
		010113	排队取药		
		010114	在线支付		
		010115	诊间结算		
		010116	患者随访		
01020	缴费结算服务	010201	医保移动支付		
		010202	商业直赔/快赔		
		010203	金融支付		
01030	转诊服务	010301	转诊服务		
01040	电子健康档案调阅服务	010401	电子健康档案调阅服务	0104011	取（查询）检查报告
				0104012	取（查询）检验报告
				0104013	取（查询）体检报告
				0104014	门急诊记录

				0104015	住院记录
				0104016	上传报告
				0104017	基本信息
				0104018	个人就诊中心
02010	妇女保健服务	020101	孕产妇建档		
		020102	孕产妇检查、随访		
		020103	出生医学证明办理		
		020104	孕期保健记录		
		020105	产检提醒		
		020106	孕期监测曲线		
		020107	孕期科普		
		0201099	其他孕产健康服务		
02020	儿童保健服务	020201	儿童体检		
		020202	疫苗接种		
		020203	预约接种记录		
		020204	儿童保健记录		
		020205	疫苗接种记录		
		020206	疫苗接种提醒		
		020207	疫苗接种证明		
		020208	儿童成长曲线		
		020209	儿童科普		
		0202099	其他儿童健康服务		
02030	慢病管理	020301	糖尿病管理		
		020302	高血压管理		
		020303	脑卒中管理		
		020304	慢病随访		
		020305	慢病科普		
		0203099	其他慢病健康服务		

02040	老年人体检管理	020401	老年人体检管理		
02050	严重精神障碍管理	020501	严重精神障碍管理		
02060	职业健康管理	020601	职业健康管理		
		020602	个人健康管理	0206021	身体指数（BMI）
				0206022	运动记录
				0206023	健康血压血糖记录
				0206024	健康饮食
				0206025	健康科普
				0206026	家庭医生
				0206027	个人健康申报
				0206028	健康状况打卡
				02060299	其他健康管理
		020603	健康评估	0206031	糖尿病评估
				0206032	高血压评估
				0206033	肿瘤风险评估
				0206034	心脑血管风险评估
02070	预防接种	020701	疫苗预约（成人）		
		020702	疫苗接种（成人）		
		020703	疫苗接种记录(成人)		
		020704	疫苗接种证明(成人)		
03010	健康精准扶贫服务	030101	健康精准扶贫服务		
03020	互联网诊疗服务	030201	互联网诊疗服务		
		030202	在线问诊	0302021	图文咨询
				0302022	视频咨询
				0302023	电话咨询
				0302024	就诊记录
				0302025	我的医生
03030	医保服务	030301	医保消费查询		

		030302	医保支付		
03040	便民服务	030401	120 急救		
03050	在线购药	030501	购药记录		
03060	抗疫服务	030601	新冠疫苗预约		
		030602	新冠疫苗接种		
		030603	新冠核酸预约		
		030604	新冠核酸检测		
		030605	疫情防疫扫码		
		030606	闸机通过扫码		
		030607	防疫数据查询		
000000	其他	000000	其他		

7.6 支付渠道编码表

父支付渠道编码	父名称	子支付渠道编码	子名称
100001	微信	10000101	微信公众号
		10000102	微信小程序
		10000103	微信 APP 支付
		10000104	H5 支付
		10000105	微信付款码支付
		10000106	扫一扫支付（主扫）
100002	支付宝	10000201	支付宝生活
		10000202	支付宝 APP 支付
		10000203	H5 支付
		10000204	支付宝小程序支付
		10000205	支付宝付款码支付
		10000206	支付宝扫一扫支付（主扫）
100003	银行卡		
100004	医保		
100005	商保		
100099	其他		

7.7 应用种类一编码表

父代码	父名称	子代码	子名称	备注
1	APP			
		101	APP Android	
		102	APP iOS	
2	微信			
		201	微信公众号	
		202	微信服务号	
3	小程序			
		301	微信小程序	
		302	支付宝小程序	
4	支付宝			
		401	支付宝生活号	
5	非医院系统			仅发卡用卡采集接口可用
		501	PC 网站	仅发卡用卡采集接口可用
		502	自助终端	仅发卡用卡采集接口可用
6	医院系统			仅发卡用卡采集接口可用
		601	His 系统	仅发卡用卡采集接口可用
		602	自助设备	仅发卡用卡采集接口可用
		699	院内其他系统	仅发卡用卡采集接口可用

7.8 应用种类二编码表

应用种类代码	应用种类名称	说明
01	预约挂号	
02	门诊就医	
03	检查检验查询	
04	互联网诊疗	
05	家庭医生签约服务	
06	基本公共卫生服务	

07	电子健康档案查询	
08	健康宣教	
09	健康体检	
10	基本医保在线支付	
11	金融移动支付	
12	健康商业险在线赔付	
13	疫情防控健康申报	
14	疫情防控核酸检测申请/查询	
15	疫情防控疫苗接种申请/查询	

7.9 发布渠道编码表

发布渠道代码	发布渠道名称	说明
100001	苹果商店	
100002	华为市场	
100003	小米市场	
100004	Vivo 市场	
100005	腾讯应用宝市场	
100006	360 手机助手市场	
100007	豌豆荚市场	
100008	Oppo 市场	
100009	魅族市场	
100010	金立市场	
100099	其他	

8 返回码

返回码	返回码描述	解决方案
0000	操作成功	
9998	交易失败	
9999	未知错误	
1001	应用编号为空	
1002	终端编号为空	
1003	不支持交易版本号	
1004	接口名称不为空	
1005	接口名称不合法	
1006	未知加密类型	
1007	未知签名类型	
1008	应用不存在	
1009	终端不存在	
1010	应用无该接口权限	
2001	电子健康卡二维码已过期	
2002	电子健康卡二维码不合法	
2003	有效时间为空	
2004	有效时间不合法	
2005	密码服务失败	
3001	无符合条件的查询记录	
3002	流水号重复	
3003	资源正在被占用，请确认交易状态再试	
8001	网络读失败	
8002	网络传输出错	
8003	空网络请求	
8004	网络连接失败	
8005	数据库连接失败	
8006	数据库配置加载失败	
8007	数据操作失败	
8008	密码服务失败	
8009	内部异常	
9001	请求参数有误	
9002	签名失败	
9003	验签失败	
9004	响应报文为空	
9005	请求系统不支持	
9006	报文加密失败	
9007	报文解密失败	
9008	报文读取错误	

附录F　（资料性）电子健康卡管理信息系统身份认证方案

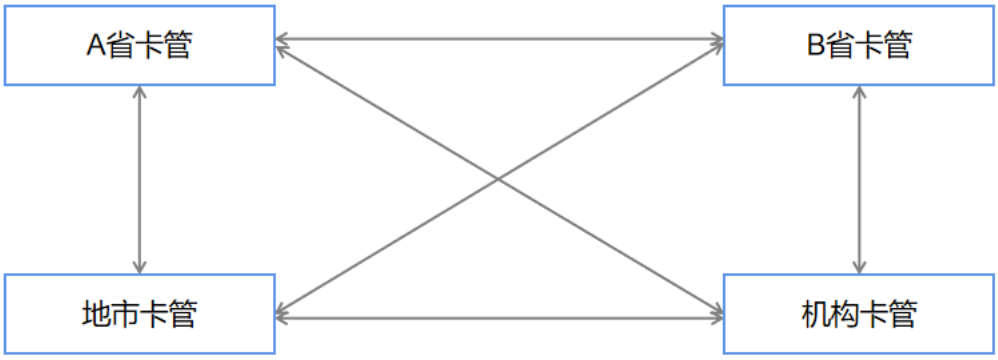
1　方案目标

本方案描述了电子健康卡管理信息系统电子认证服务体系中数字证书互认架构、数字证书格式、密码算法、网络安全和数据保护方法，在电子健康卡管理信息系统内通过数字证书互信互认，实现了身份认证、数据完整性、抗抵赖和机密性保护。

2　总体架构

本部分规定了基于国产密码算法使用电子健康卡管理信息系统身份认证与系统鉴权管理开展电子健康卡管理信息系统的使用，实现电子健康卡管理信息系统电子认证服务体系标准化调用，减少因接口不兼容所引起的重复开发工作和安全性问题，提高应用软件的通用性和可移植性，降低应用系统安全风险。

本部分适用于电子健康卡管理信息系统按照本部分进行安全开发与使用。



卡管系统在注册后完成订阅和互认，使用数字证书实现：
1. 身份认证　2. 数字签名　3. 数据加密　4. 可信时间戳

上图所示，根据电子健康卡跨域认证服务体系架构，本级卡管节点通过跨域认证服务的全网节点路由信息，实现在应用节点和发卡节点间进行跨域认证。本方案以不额外增加认证体系为原则，在原有认证服务体系的基础上，依据现有信息流转模式，在卡管注册时同步注册本级卡管公钥证书、根证书及 CRL 策略，通过订阅流程同步卡管路由信息、公钥证书、根证书及 CRL 策略。 配合密码设备，实现各级卡管系统之间的身份认证、信息完整性保护、保密传输和防抵赖功能。

3 卡管系统间网络通讯和数据安全

为每个卡管节点签发数字证书，并参照以下要求：

(1) 应采用数字证书对卡管系统进行身份鉴别，保障卡管系统的真实性；

(2) 宜采用数字证书保证通信数据和业务报文的完整性；

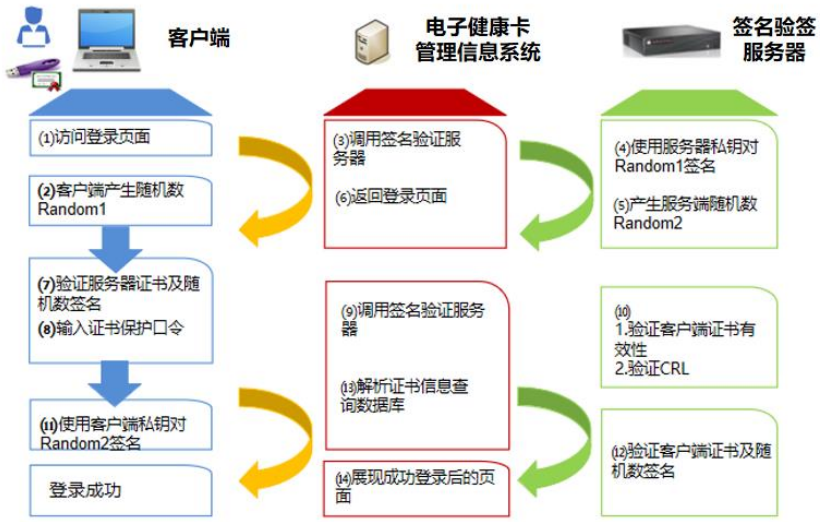
(3) 应采用密码技术和数字证书保证通信数据和业务报文的机密性。

4 卡管系统管理员身份认证

4.1 实现方式 1

身份认证主要针对个人用户通过使用智能密码钥匙，访问电子健康卡管理信息系统时所需要的基于数字证书进行的强身份鉴别。

身份认证接口由服务端接口和客户端接口两部分组成。服务端接口为报文模式，应用系统根据约定的报文格式组织、发送、解析报文；客户端接口以动态链接库或 JS 脚本的形式存在，加载在被改造应用的客户端或认证页面中。



身份认证流程

(1) 个人用户访问卡管系统页面；

(2) 客户端产生随机数 Random1；

(3) 卡管系统调用签名验证服务器；

(4) 签名验证服务器对 Random1 做签名，并产生随机数 Random2；

(5) 卡管系统返回随机数 Random2、随机数 Random1 的签名及服务器证书；

(6) 客户端对服务器证书和随机数签名进行验证；

(7) 卡管系统调用签名验证服务器，验证客户端证书的有效性；

(8) 用户输入客户端证书保护口令，客户端对随机数 Random2 签名；

(9) 获取客户端证书、随机数 Random2 的签名后调用签名验证服务器对其进行验证，完成认证过程；

(10)验证通过后，卡管系统解析客户端证书，获取其唯一标识；查询业务数据库进行用户身份匹配，匹配成功后展现登录成功页面。

4.2 实现方式 2

管理员和操作员访问电子健康卡管理信息系统，卡管系统将请求重定向至认证网关，认证网关与客户端之间建立安全传输通道并对客户端证书进行有效性认证，认证结果返给卡管系统。卡管系统根据认证网关返回的认证结果判断是否让用户登录。

5 策略和要求

电子认证服务机构互信互认应遵循以下规范：

- 《中华人民共和国电子签名法》
- 《卫生系统电子认证服务规范(试行)》
- 《卫生系统数字证书格式规范》
- 《卫生系统数字证书介质规范》
- 《卫生系统数字证书应用集成规范》
- 《GM/T 0010 SM2 密码算法加密签名消息语法规范》
- 《GM/T 0029-2014 签名验签服务器技术规范》
- 《GM/T 0033-2014 时间戳接口规范》
- 《GM/T 0024-2014 SSL VPN 技术规范》
- 《GM/T 0025-2014 SSL VPN 网关产品规范》

- 《GM/T 0026-2014 安全认证网关产品规范》

5.1 数字证书跨域认证策略

不同 CA 机构签发的数字证书通过根证书互认，实现不同 CA 机构证书的互认互验，例如，首先验证数字签名，然后验证公钥证书的证书链，最后验证公钥证书的时间有效性，是否被吊销。

5.2 数字证书算法

(1) 采用 SM2 国密数字证书。

(2) 数字签名采用 SM2WithSM3 国密算法。

(3) 数字信封采用 SM2WithSM4 国密算法。

数字签名和数字信封算法应满足“GM/T 0010 SM2 密码算法加密签名消息语法规范”中所述规定，以实现技术层面的互通互认。

6 参考文献

- 《GBT+22239-2019 信息安全技术 网络安全等级保护基本要求》
- 《GB_T 39786-2021 信息安全技术 信息系统密码应用基本要求》

《电子健康卡建设与管理指南》材料二

电子健康卡质量控制与安全运行管理要求

（2.2 版）

国家卫生健康委统计信息中心

2022 年 3 月

目　录

电子健康卡质量控制与安全运行管理要求

本部分给出了电子健康卡建设、运行的基本流程和步骤，并提出了各环节中质量控制和安全运行管理的要求。主要内容包括电子健康卡质量管理基本要求、电子健康卡系统平台建设流程要求、电子健康卡运行管理要求等。

1　电子健康卡质量管理基本要求

1.1 产品标准符合性要求

为确保电子健康卡标准统一、全国通用、安全运行，建设单位应选择符合电子健康卡标准的产品（包括电子健康卡管理信息系统、电子健康卡密码模块、电子健康卡识读终端、客户端应用软件等），产品生产商应提供产品与《电子健康卡技术规范》要求一致性的证明材料。

国家卫生健康委统计信息中心建立质量监督机制，每年度组织专业力量对建设单位所使用的电子健康卡系统平台（包括电子健康卡管理信息系统、电子健康卡密码模块、电子健康卡识读终端、客户端应用软件等）按照一定比例进行抽查，以确认实际应用的产品是否满足本指南和《电子健康卡技术规范》的要求。

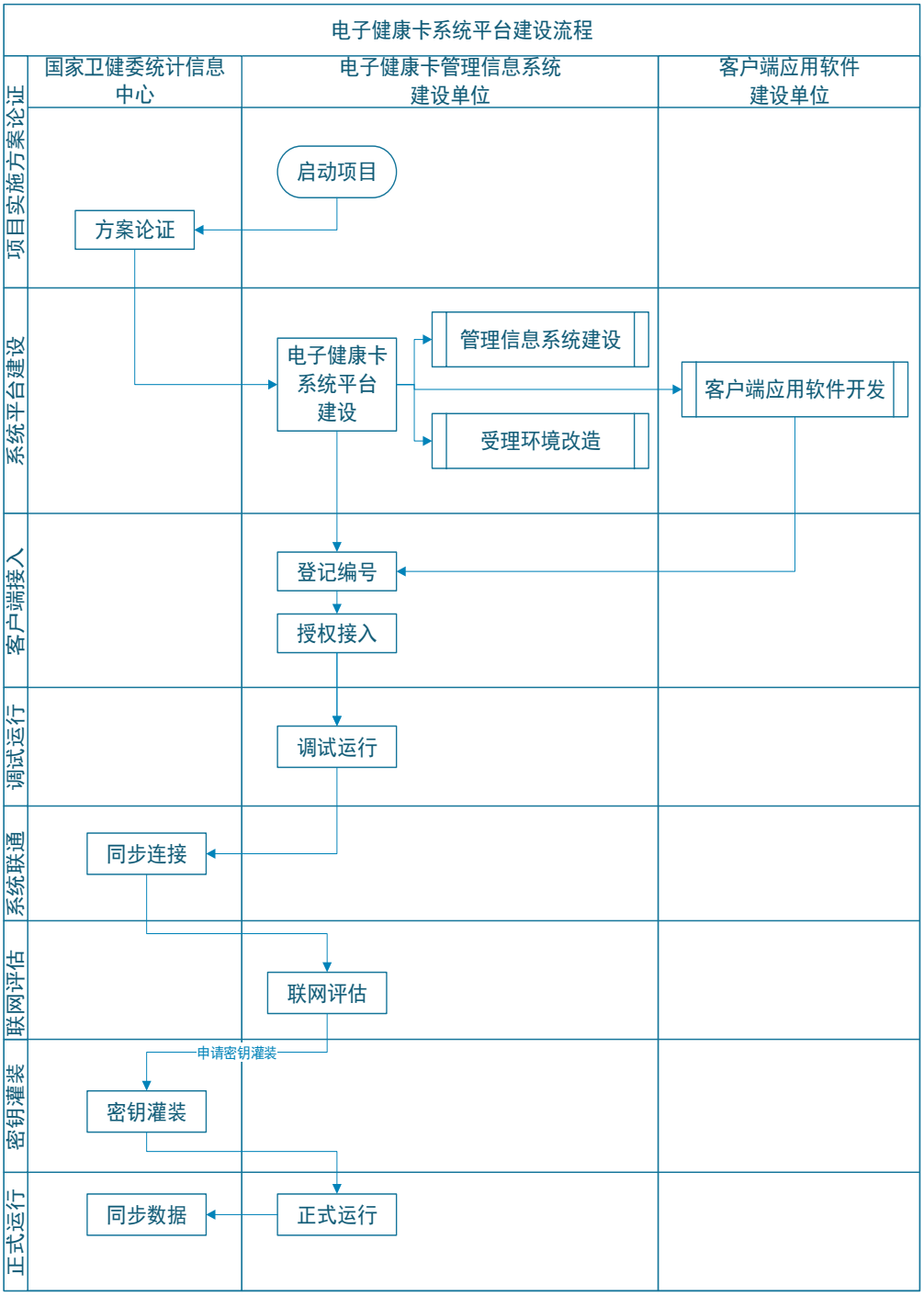
1.2 电子健康卡网络安全责任

各建设单位的电子健康卡系统平台与国家电子健康卡系统平台共同组成全国电子健康卡网络。电子健康卡网络中所有的节点实行登记管理，各区域网络登记入网节点信息。各级区域系统的运行单位负责本区域的网络安全建设和管理工作。

2　电子健康卡系统平台建设流程要求

电子健康卡是基于统一标准进行设计的、能够实现全国联网通用的“就诊卡”。为保障电子健康卡系统平台建设的满足电子健康卡的设计要求，需要对电子健康卡的整体建设流程进行规范管理。

建设流程总体如下：



2.1 项目备案申请

电子健康卡系统平台的建设单位，应首先应向国家卫生健康委统计信息中心申领国家居民健康卡综合管理平台数字证书，再在线进行平台账号注册。申请数字证书要求及方式在平台首页“通知公告”中“数字证书管理办法”中写明。账号注册成功后，在平台中进行电子健康卡项目备案申请。

2.2 项目实施方案论证

2.2.1 实施方案

电子健康卡系统平台的建设单位，应制定本单位的电子健康卡建设方案。建设方案至少应包含本单位对电子健康卡系统平台的基本认识，对电子健康卡系统平台建设的时间安排，电子健康卡系统平台的网络架构设计、应用系统设计，电子健康卡系统平台的应用场景设计，电子健康卡系统平台的安全保障设计，以及电子健康卡系统平台建设的参与方和投入保障等内容。

2.2.2 方案论证与备案

电子健康卡建设方案应由国家卫健委统计信息中心组织专家进行统一评审。省级电子健康卡建设方案已通过论证的省份，在省内扩展市级或医院应用试点或者分级部署时，可由省级自行组织专家进行论证。未通过论证的方案，应根据专家意见进行修改，不能作为电子健康卡系统平台建设的依据。

通过论证的建设单位应在系统平台建设前上传《电子健康卡项目建设方案》和《修订版电子健康卡项目建设方案》、审核单位上传《建设方案专家论证意见》和《专家名单》至国家居民健康卡综合管理平台。省级自行组织论证的建设方案在备案时，应关联已通过评审的省级电子健康卡建设方案。

2.3 系统平台建设

电子健康卡系统平台的建设单位，应按照《电子健康卡建设与管理指南》进行系统建设。电子健康卡系统平台建设内容包括：

（1） 选用符合《电子健康卡技术规范 2-4 部分》要求的电子健康卡管理信息系统、电子健康卡密码模块、电子健康卡识读终端；

（2） 接入电子健康卡的客户端应用软件，包括 APP、第三方服务号、自助终端及其它类型的终端等；

（3） 改造电子健康卡的受理应用环境，实现电子健康卡在业务应用机构的场景落地。

电子健康卡系统平台建设时，应选择具有一定实力的生产商，保证电子健康卡系统平台的可靠性。电子健康卡系统平台的建设单位应要求生产商提供产品与《电子健康卡技术规范》要求一致性的证明材料，促进产品合规、互联互通的能力。

2.4 客户端应用软件接入

建设单位应对接入电子健康卡管理信息系统的客户端应用软件实行登记制度。

客户端应用软件开发完成后，在上线之前，建设单位应向其准备接入的电子健康卡管理信息系统进行注册登记，并按照《电子健康卡密码模块接口及卡管系统接入认证技术要求》的接入组件编码规则分配登记编号。APP Android、APP iOS、公众号、服务号等每个应用种类均应分配登记编号。

电子健康卡客户端应用软件在登记时，应提供电子健康卡客户端应用软件符合《电子健康卡技术规范 第 5 部分：客户端应用软件》中功能、安全、接口、UI、稳定性、性能效率等方面要求的证明材料。

客户端发生重大版本变更（大版本变更是指版本 x.y 的 x 或 y 发生变化）时，建设单位应向电子健康卡管理信息系统报备版本变更情况。建设单位对客户端应用软件在运行过程中的安全负责，保障电子健康卡健康、有序地推广和普及。客户端发生重大版本变更时，建设单位应重新进行安全评估，保证其持续的安全性。

国家卫健委统计信息中心将汇总并公示已取得登记编号的电子健康卡客户端应用软件，省级卫健委应同步公示本省管辖范围内的有效电子健康卡客户端应用软件。

2.5 系统平台调试运行

电子健康卡客户端应用软件接入电子健康卡管理信息系统后，建设单位可使用模拟密钥开展电子健康卡系统平台的调试运行工作，并且应通过电子健康卡管理信息系统实现客户端应用软件的接入管理。

调试运行工作主要验证电子健康卡在实际生产环境中的可用性，检验电子健康卡在发行、受理各个环节的运行效果，帮助建设单位及时发现问题。

2.6 系统平台联通

建设单位应确保各地电子健康卡管理信息系统与国家电子健康卡应用监测系统和电子健康卡跨域主索引及跨域认证系统建立持续的接口心跳关系，保证数据接口互通。

2.7 联网评估

为保障全国电子健康卡网络体系的安全，在密钥灌装前，电子健康卡系统平台应按照《电子健康卡技术规范 第 6 部分：运行环境》进行联网评估。

电子健康卡系统平台的建设单位建设单位可选择自评估或第三方检测机构评估的方式，

出具联网评估报告；联网自评估应确保评估方法的有效性，并对评估结果的真实性和准确性做出有效承诺（承诺函参考模板见附录 A），对评估发现的风险及问题应进行及时整改或制定有效的措施降低风险，并形成加盖公章的评估报告。承诺函及自评估报告模板可在国家居民健康卡综合管理平台中自行下载。

为保证电子健康卡系统平台的风险处于可控范围内，建设单位应建立定期评估的安全机制。

2.8 密钥灌装及密码模块管理

电子健康卡系统平台调试运行贯通全部业务环节后，电子健康卡系统平台的建设单位在国家居民健康卡综合管理平台中提出密钥灌装申请，加入全国电子健康卡网络体系。

各建设单位需在密钥灌装申请时首先上传电子健康卡管理信息系统、电子健康卡密码模块、电子健康卡识读终端、客户端应用软件的产品资质声明、接入声明等声明材料。建设单位可请第三方检测机构进行检测，并上传相应检测报告至国家居民健康卡综合管理平台；建设单位也可采用自评估方式，须填写承诺函，对电子健康卡系统平台的质量、合规性和运行安全负责，声明材料包括“承诺函”、“产品自评估报告”、“接入自评估报告”、“联网自评估报告”、“软件著作权登记证书”、“商用密码产品型号证书”等材料至国家居民健康卡综合管理平台（参考模板见附录 A-F）。

满足联网评估要求的电子健康卡系统平台，由国家卫健委统计信息中心许可入网并向电子健康卡密码模块下发正式密钥。密码模块的信息应登记在电子健康卡管理信息系统中。正式密钥灌装后，建设单位启动电子健康卡系统平台的正式运行。

需再次密钥灌装的，如电子健康卡系统平台部署环境未发生改变，可在国家居民健康卡综合管理平台中在初次密钥灌装的项目基础上再次申请密钥灌装；如电子健康卡系统平台部署环境发生改变，需重新进行联网评估后申请密钥灌装。

若已灌装密钥的密码模块拟停止使用需要在国家居民健康卡综合管理平台上提交停止使用申请，并上传已清除电子健康卡密钥的工作证明：该设备不再使用，可采用物理销毁的方法来删除密钥；如该设备仍将继续使用，可采用覆盖重写的方法删除密钥。

2.9 系统平台正式运行

电子健康卡系统平台的建设单位应加强电子健康卡系统平台运行过程中的技术管理工作，确保电子健康卡系统平台满足《电子健康卡建设与管理指南》的相关要求，保持电子健

康卡管理信息系统与国家电子健康卡应用监测系统和电子健康卡跨域主索引及跨域认证系统的持续互联互通，建立心跳联系，保证数据及时上传和调用。

3 电子健康卡运行管理要求

3.1 电子健康卡系统平台运行管理要求

电子健康卡系统平台的建设单位对电子健康卡系统平台的稳定、可靠、安全运行承担最终责任。

建设单位应确保电子健康卡建设相关组件，包括电子健康卡管理信息系统、电子健康卡密码模块、电子健康卡识读终端、客户端应用软件等符合《电子健康卡技术规范》相关要求，保障电子健康卡质量，以便实现电子健康卡的跨域认证、互联互通。

建设单位可选择具有检测资质以及检测服务能力的第三方检测机构或者自行进行相关技术要求确认工作。自行进行技术确认工作的，建设单位须填写承诺函，承诺其实际应用的相关组件满足本指南和《电子健康卡技术规范》的要求。承诺函参考模板见附录 B-F。

建设单位应保障电子健康卡的运行维护投入，确保电子健康卡管理信息系统持续满足《电子健康卡建设与管理指南》的要求，并符合网络安全等级保护第三级的安全要求，及符合商用密码应用安全性评估要求。建设单位应指导接入电子健康卡管理信息系统的机构，要求其接入的系统按照同等级的安全标准进行建设；尤其是电子健康卡客户端应用软件的运营机构，应按照《电子健康卡建设与管理指南》的要求，加强客户端应用软件自身的安全开发工作，在客户端应用软件的版本更新过程中，始终遵循安全标准的要求。

电子健康卡系统平台的建设单位对电子健康卡系统平台的运行负责。建设单位应采取有效地措施，保证电子健康卡系统平台的标准符合性和安全性，建立长效机制，监督和管理接入电子健康卡管理信息系统的客户端应用软件安全。

3.2 运行安全风险控制

加强常态安全风险监控机制建设，对管辖范围内的电子健康卡客户端应用软件运行情况实时掌控，以满足网络安全部门在移动应用安全方面政策性和合规性要求，形成行业内部安全风险控制和修复、自检自查自律的基本能力，促进互联网医疗产业的健康发展，增强公众的使用信心。

建设单位及客户端应用软件的运营单位应加强电子健康卡管理信息系统及客户端应用

软件的安全保障体系建设，建立健全电子健康卡用卡过程监测和有关安全风险动态评估管理机制，通过主动、持续、动态的风险业务识别、侦测和分析，达到风险识别、预警、处置的风险闭环控制，为电子健康卡“线上线下一体化”医疗健康服务应用提供安全保障支撑，确保居民健康信息安全。

登记编号未在客户端应用软件中标识、不在公示列表范畴、注册登记不完整（如只注册安卓版本但实际发布安卓及苹果版本）、发布渠道中存在盗版应用、登记版本与流通版本存在大版本差异、安全等级较低（根据移动应用安全风险高低情况进行动态安全评分）等情况均应在客户端应用软件运行过程中进行实时监管。

建设单位应建立事前登记管理、事中监管、事后通告的机制，当客户端应用软件出现安全问题时，及时进行相应处置，避免扩大安全影响。

客户端应用软件的运营单位应为用户安全、便捷地使用客户端应用软件负责，应采取有效手段，主动、持续、动态地预防客户端应用软件的安全风险和业务风险。

建议客户端应用软件运行过程中的问题处置措施如下：

1、 对于登记编号未在客户端应用软件中标识、不在公示列表范畴、注册登记不完整（如只注册安卓版本但实际发布安卓及苹果版本）等情况，将视为违规应用，原则上应暂停接入电子健康卡管理信息系统，待取得登记编号后方可予以接入。

2、 在运行中发现盗版、近似应用等非法客户端应用软件时，建设单位或者运营单位应进行自查自纠。

3、 在运行中发现实际运行版本与接入登记版本存在大版本（大版本变更是指版本 x.y 的 x 或 y 发生变化）差异时，原则上该应用应暂停接入电子健康卡管理信息系统，进行登记更新后再行接入。

附录A　电子健康卡联网检测现场自评估报告和承诺函模板

电子健康卡联网评估承诺函

我单位：XX，严格按照《电子健康卡建设与管理指南》和《电子健康卡技术规范 第6部分：运行环境》要求，以第三方检测机构评估/自评估方式进行联网评估，评估结果符合要求；我单位已通过网络安全等级保护测评，系统达到第三级要求，并已通过商用密码应用安全性评估。/我单位承诺于xx年xx月完成网络安全等级保护三级测评和商用密码应用安全性评估。

我单位承诺保证电子健康卡管理信息系统直接与国家级系统联通，建立接口持续的心跳关系，保证数据的及时上传，实现电子健康卡管理信息系统与国家级系统的数据同步，实现各地用卡情况的有效监测。

单位负责人签字：

（单位盖章）

日　　期：

电子健康卡联网检测
现场自评估报告

自评估单位信息	
自评估单位名称 （单位盖章）	
联　系　人	
联 系 电 话	
电 子 邮 件	

目录

1 名词术语

表 1.1 名词术语

序号	名词术语	相关解释
（1）	电子健康卡	可通过二维码形式展现为电子健康卡，功能与实体居民健康卡相同。
	电子健康卡管理信息系统	在电子健康卡注册用卡过程中，负责电子健康卡发卡数据的生产、使用和管理，采用电子账户对信息进行存储，并支持线下交互的技术应用。
	主索引 ID	是标识居民健康卡用户唯一性的信息，通过主索引 ID 关联用户的实体居民健康卡、电子健康卡、医院就诊卡等不同类型账户。
	电子健康卡 ID	电子健康卡管理系统用于标识电子健康卡账户唯一性的信息，电子健康卡 ID 由用户的证件类型和证件号码的密文组成。
	电子健康卡二维码	电子健康卡通过二维码的形式予以展示，通过“面对面”方式进行交互使用。电子健康卡二维码包括静态二维码和动态二维码：静态二维码可通过移动 APP 呈现，也可印刷或粘贴于就诊卡等介质上，适用于挂号、问诊等非核心应用场景；动态二维码由 APP 呈现，在每次使用前生成，其生命周期根据应用安全的要求限定时间范围，适用于病历查询、结算交易等核心应用场景。
	密码设备	密码设备是具有某种密码功能或能完成某种密码工作任务的设备的统称。
	接入机构	接入使用电子健康卡管理信息系统，与平台提供接口存在交互逻辑的相关机构事业单位，包括但不限于医疗卫生机构、医保机构等。
	接入 APP	接入电子健康卡管理信息系统，与平台接口存在交互逻辑的互联网移动应用软件。
	电子健康卡 API 接口	是泛指远程连接到电子健康卡管理系统的 API 接口，主要完成电子健康卡的注册、二维码申请、二维码验证等功能，接入 APP 通过 API 接口连接电子健康卡管理系统。
	识读终端	识读二维码并与后台应用系统进行交互的终端，一般包括二维码的识读设备和终端机上的应用软件。

2 引用文档

2.1评估标准

1) 《电子健康卡建设与管理指南（试用）》；

2) 《电子健康卡技术规范 第 6 部分：运行环境》。

2.2参考资料

3 评估资源

3.1系统环境

系统拓扑图如下。

图 4.1 系统拓扑图

3.2主要设备

主要设备包括：网络设备、主机、密码机、识读终端
本次评估主要设备如下表：

表 3.2 主要设备列表

设备名称	规格型号	数量	备注

3.3评估设备

评估所使用工具/设备如下：

表 3.3 评估设备列表

软件/设备名称	版本号/型号	生产商	用途
评估设备应包括性能测试工具、系统扫描工具、网络设备和主机扫描工具，及功能评估辅助设备			

4 相关说明

4.1评估结果判定

- 符合：评估结果既符合评估依据的要求。
- 不符合：评估过程中发现问题未整改或整改后评估结果为不符合评估依据的要求。
- 整改符合：评估过程中发现问题经整改后评估结果为符合评估依据的要求。

4.2评估结论判定

- 通过：所有必选项均符合或整改符合评估依据的要求则总结论为通过。
- 不通过：任何必选项评估不符合则总结论为不通过。

5 评估内容及结果

说明：现场评估所有评估项为必选项。

现场评估功能性共 12 项，通过整改全部符合/全部符合；性能效率共 3 项，全部符合；信息安全性共 28 项，符合 xx 项，不符合 xx 项；接口共 10 项，通过整改全部符合；系统灾备共 7 项，全部符合；管理要求共 29 项，通过整改全部符合；具体评估内容及结果见下表。

5.1 功能性

表 5.1 功能评估内容及结果

序号	评估项	评估要求	评估方法及步骤	评估结果	结果判定	整改措施
1.	电子健康卡管理信息系统系统版本	电子健康卡管理信息系统已经通过质量确认的，系统应是通过质量确认版本或高于通过质量确认（版本更新应有版本更新记录说明）。	查看系统版本，如有更新检查更新记录说明。	应描述评估结果 例：电子健康卡管理信息系统与实验室通过检测版本相同	**符合/整改符合/不符合**	
2.	电子健康卡管理信息系统用户管理	系统自身具有用户管理以及用户权限管理功能。	检查系统管理权限配置功能。	例：系统具有用户管理及用户权限管理相关功能	**符合/整改符合/不符合**	
3.	密码设备接入	密码设备是通过质量确认的型号，密码设备高	检查密码设备型号和版本。			

序号	评估项	评估要求	评估方法及步骤	评估结果	结果判定	整改措施
	许可	级应用编程接口与通过质量确认版本一致。				
4.	密码设备验证	电子健康卡管理信息系统已对接密码设备，断开密码设备业务不能正常使用。	断开密码设备验证。			
5.	密码负载均衡	2 台（含）以上密码设备和电子健康卡管理信息系统连通性，实现负载均衡。	检查密码设备部署拓扑，并验证是否实现负载均衡模式。			
6.	密码设备生成数据一致性	密钥灌装后，在现场使用一组用户信息（姓名和身份证）生成一组数据，是否和密钥灌装时一致。（密钥灌装后验证）	现场环境使用一组用户信息（姓名和身份证）生成一组数据，生成输出的数据应和密钥灌装时一致。			
7.	识读终端接入许可	识读终端是通过质量确认的型号。	检查识读终端型号。			
8.	客户端应用APP/微信公众号/支付宝服务号接入许可	APP、微信公众号、支付宝服务号应该具有客户端应用软件接入质量要求说明。	检查互联网终端接入质量要求说明情况。			
9.	授权接入	客户端应用软件应采用电子健康卡管理信息系统接入层认证方案要求与卡管系统进行授权接入	检查客户端应用软件与卡管系统采用授权接入认证报文			
10.	全流程展示验证	是应用场景对关键业务（医院就诊全流程）的实现。包括医院窗口二维码领取就诊、手机终端二维码就诊、医院自助终端流程。	在医院模拟就诊全流程。			
11.	电子健康卡管理信息系统联	电子健康卡管理信息系统与省级系统联通。	检查电子健康卡管理信息系统与省级系统的联通情况。			
12.		电子健康卡管理信息系	检查电子健康卡管			

序号	评估项	评估要求	评估方法及步骤	评估结果	结果判定	整改措施
	通管理	统与国家电子健康卡应用监测系统。	理信息系统与国家电子健康卡应用监测系统的联通情况。			
13.		电子健康卡管理信息系统与电子健康卡跨域主索引及跨域认证系统联通。	检查电子健康卡管理信息系统与电子健康卡跨域主索引及跨域认证系统的联通情况			

5.2　性能效率

表 5.2 性能效率评估内容及结果

序号	评估项	评估要求	评估方法及步骤	自评估结果	结果判定	整改措施
1.	电子健康卡管理信息系统	用户注册多用户并发成功率 100%；单笔交易响应时间不超过 1s 。	使用软件工具或测试工具箱开发脚本模拟真实用户访问场景进行并发测试。	每秒最大完成请求数应高于区域人口数的千分之一，扩容后应满足区域人口数的千分之二，成功率 100%；单笔交易响应时间不超过 1s 。		
		性能结果截图 **（截图中应展示测试脚本内容和相应测试结果内容）**				
2.		二维码生成多用户并发成功率 100%； 单笔交易响应时间不超过 1 秒。	使用软件工具或测试工具箱开发脚本模拟真实用户访问场景进行并发测试。	每秒最大完成请求数应高于区域人口数的千分之一，扩容后应满足区域人口数的千分之二，成功率 100%；单笔交易响应时间不超过 1s 。		
		性能结果截图				
3.		二维码验证多用户并发成功率 100%； 单笔交易响应时间不超过 1 秒。	使用软件工具或测试工具箱开发脚本模拟真实用户访问场景进行并发测试。	每秒最大完成请求数应高于区域人口数的千分之一，扩容后应满足区域人口数的千分之二，成功率 100%；单笔交易响应时间不超过 1s 。		
		性能结果截图				

5.3 信息安全性

5.3.1 系统安全

表 5.3.1 系统安全评估内容及结果

序号	评估项	评估要求	评估方法及步骤	自评估结果	结果判定	整改措施
1.	系统扫描	电子健康卡管理信息系统进行安全漏洞扫描检测，未存在高、中级别安全风险。	使用软件工具或测试工具箱进行扫描测试。	应提供测试工具名称及版本号		
2.	访问控制	电子健康卡管理信息系统的应用服务器和数据库服务器位于内部网络区域，与互联网之间有 DMZ 区隔离。	检查网络拓扑图和数据环境。			
3.		电子健康卡管理信息系统的管理人员终端专属运维终端，与互联网进行隔离。	访谈管理人员并检查管理终端。			
4.		电子健康卡管理信息系统的管理人员拥有独立的账户，非管理人员未授权不能访问。	访谈管理人员并检查账户使用情况。			
5.		系统的管理人员终端安装了防病毒软件。	访谈管理人员并检查管理终端。			
6.	通信安全	电子健康卡管理信息系统对互联网、专网提供的服务（手机客户端、微信等），通信应是安全的。（通讯安全手段如加密协议、ipsec vpn 等手段。）	现场检查并评审电子健康卡管理信息系统对互联网提供的通信安全措施。			
7.		APP 终端/微信公众号/支付宝服务号的后台服务器通信应是安全的。（通讯安全手段如：加密协议、ipsec vpn 等手段。）	检测并验证 APP 终端/微信公众号/支付宝服务号的后台服务器提供的安全通信情况。			
8.	系统防护	系统防护策略包括： 删除或者禁用不使用的账户； 限制密码长度（推荐 8	检查并验证系统对账户的安全管理机制。			

序号	评估项	评估要求	评估方法及步骤	自评估结果	结果判定	整改措施
		位及以上）； 设置密码复杂度（包含字母和大小写数字）； 限制密码使用期限（90天强制修改密码）； 设置访问空闲超时（推荐10分钟）。				

5.3.2 网络安全

表 5. 3. 2 网络安全评估内容及结果

序号	评估项	评估要求	评估方法及步骤	自评估结果	结果判定	整改措施
1.	网络扫描	对网络设备进行安全漏洞扫描检测，未存在高、中级别安全风险。	使用软件工具或测试工具箱进行扫描测试。	应提供测试工具名称及版本号		
2.	结构安全	绘制与当前运行情况相符的网络拓扑结构图。	检查网络拓扑图，现场查验和实际网络环境一致。			
3.		根据各部门的工作职能、重要性、所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。	检查各网段分配和区域划分情况。			
4.		重要网段应采取网络层地址与数据链路层地址绑定措施，防止地址欺骗。	检查安全设备绑定配置，并验证配置。			
5.	访问控制	能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级。	检测并验证网络设备对用户访问权限的控制。			
6.		会话处于非活跃一定时间或会话结束后终止网络连接。	检测并验证网络设备对用户访问权限的控制。			
7.		限制网络最大流量数及网络连接数。	检测并验证网络设备对用户访问权限的控制。			
8.	安全审计	对网络系统中的网络设备运行状况、网络流	检查网络设备安全审计功能情况。			

序号	评估项	评估要求	评估方法及步骤	自评估结果	结果判定	整改措施
		量、用户行为等进行全面的监测、记录。				
9.		可以根据记录数据进行分析，并生成审计报表。	操作审计日志可以导出报表。			
10.	入侵防范	在互联网边界区域部署防火墙等安全设备进行防护，防护的策略是有效的。	1、检查网络边界防火墙。 2、使用工具测试验证防火墙策略有效性。			
11.		在关键网络节点部署IPS/IDS等入侵防范设备进行入侵防范，防护的策略是有效的。	1、检查关键网络节点是否部署IPS/IDS设备。 2、使用工具测试验证入侵防护策略有效情况。			
12.		在关键网络节点部署防DDoS攻击的设备，防护的策略是有效的。	1、检查关键网络节点部署DDOS设备情况。 2、使用工具测试验证入侵防护策略有效情况。			
13.	设备防护	网络设备防护策略包括： 删除或者禁用不使用的系统缺省账户； 限制密码长度（推荐8位及以上）； 设置密码复杂度（包含字母和大小写数字）； 限制密码使用期限（90天强制修改密码）； 设置访问空闲超时（推荐10分钟）； 默认管理员账户未授权不能远程登录设备。	检查并测试验证系统对账户的安全管理机制。			

5.3.3 主机安全

表 5.3.3 主机安全评估内容及结果

序号	评估项	评估要求	评估方法及步骤	自评估结果	结果判定	整改措施
1.	主机扫	对主机系统进行安全漏	使用软件工具或测			

序号	评估项	评估要求	评估方法及步骤	自评估结果	结果判定	整改措施
	描	洞扫描检测，未存在高、中级别安全风险。	试工具箱进行扫描测试。			
2.	主机防护	主机防护策略包括： 删除或者禁用不使用的系统缺省账户； 限制密码长度（推荐 8 位及以上）； 设置密码复杂度（包含字母和大小写数字）； 限制密码使用期限（90 天强制修改密码）； 设置访问空闲超时（推荐 10 分钟）； 默认管理员账户未授权不能远程登录设备。	检查并测试验证系统对账户的安全管理机制。			
3.	病毒防范	服务器和终端设备（包括移动设备）均应安装实时检测和查杀病毒的软件产品。	检查主机服务器安装查杀病毒的软件产品情况并记录。			

5.3.4 物理安全

表 5. 3. 4 物理安全评估内容及结果

序号	评估项	评估要求	评估方法及步骤	自评估结果	结果判定	整改措施
1.	物理位置	电子健康卡管理信息系统和密码设备的位置与应用服务器处于同一区域。	检查电子健康卡管理信息系统和密码设备的位置。			
2.		机房应选择在具有防震、防风和防雨等能力的建筑内。	检查机房场所。			
3.	防破坏	通信线缆铺设在隐蔽处，如铺设在地下或管道中等。	检查机房场所。			
4.	访问控制	对重要区域配置电子门禁系统，鉴别和记录进入的人员身份并监控其活动。	检查机房场所。			

5.4 接口

表 5. 4 接口评估内容及结果

序号	接口项	质量要求	确认方法及步骤	预期结果及判定	质量说明
1.	识读终端接口	识读业务接口正常使用。	检查识读接口并验证识读情况	具有识读接口并能识读	**必选项**
2.	APP 接口/微信公众号/支付宝服务号	APP 接口/微信公众号/支付宝服务接口正常使用。	检查第三方接口并验证联通情况	具有第三方接口并能联通	**必选项**
3.	机构连接接口	机构业务接口正常使用。	检查结构接口并验证联通情况	具有机构接口并能联通	**必选项**
4.	密码模块接口	密码模块接口可正常使用。	检查密码模块接口并验证联通情况	具有密码模块接口并能联通	**必选项**
5.	用户注册	用户注册接口可正常使用。	检查注册接口并验证注册数据	具有注册接口并能注册	**必选项**
6.	二维码生成	二维码生成接口可正常使用。	检查生成接口并验证生成数据	具有生成接口并能生成	**必选项**
7.	二维码验证	二维码验证接口可正常使用。	检查验证接口并验证验证数据	具有验证接口并能验证	**必选项**
8.	用卡监测平台接口	用卡监测平台业务接口可正常使用。	检查用卡监测接口并验证联通情况	具有用卡监测接口并能联通	**必选项**
9.	跨域主索引接口	国家平台业务接口可正常使用。	检查跨域主索引接口并验证联通情况	具有跨域主索引接口并能联通	**必选项**
10.	跨域认证服务接口	跨域认证服务接口可正常使用	检查跨域认证服务接口并验证联通情况	具有跨域认证服务接口并能联通	**必选项**

序号	评估项	评估要求	评估方法及步骤	自评估结果	质量说明
1.	识读终端接口	识读业务接口正常使用。	检查识读接口并验证识读情况		**必选项**
2.	APP 接口/微信公众号/支付宝服务号	APP 接口/微信公众号/支付宝服务接口正常使用。	检查第三方接口并验证联通情况		**必选项**
3.	机构连接接口	机构业务接口正常使用。	检查结构接口并验证联通情况		**必选项**
4.	密码模块接口	密码模块接口可正常使用。	检查密码模块接口并验证联通情况		**必选项**
5.	用户注册	用户注册接口可正常使用。	检查注册接口并验证注册数据		**必选项**
6.	二维码生成	二维码生成接口可正常使用。	检查生成接口并验证生成数据		**必选项**
7.	二维码验证	二维码验证接口可正常使用。	检查验证接口并验证验证数据		**必选项**
8.	用卡监测平台接口	用卡监测平台业务接口可正常使用。	检查用卡监测接口并验证联通情况		**必选项**

9.	跨域主索引接口	国家平台业务接口可正常使用。	检查跨域主索引接口并验证联通情况		**必选项**
10.	跨域认证服务接口	跨域认证服务接口可正常使用	检查跨域认证服务接口并验证联通情况		**必选项**

5.5 系统灾备

表 5.5 系统灾备评估内容及结果

序号	评估项	评估要求	评估方法及步骤	自评估结果	结果判定	整改措施
1.	电子健康卡管理信息系统	电子健康卡管理信息系统应用服务器具有冗余机制，并验证有效性。	检查冗余机制并验证。			
2.		电子健康卡管理信息系统数据库服务器具有冗余机制，并验证有效性。	检查冗余机制并验证。			
3.		电子健康卡管理信息系统和数据具有备份和恢复策略，对关键数据定期备份，备份数据应保密并有专人管理。	检查备份和恢复策略以及备份是否有专人管理。			
4.	网络设备	防火墙设备具有冗余机制，并验证有效性。	检查冗余机制并验证。			
5.		交换机设备具有冗余机制，并验证有效性。	检查冗余机制并验证。			
6.	密码设备	密码设备具有冗余机制，并验证有效性。	检查冗余机制并验证。			
7.	其他网络设备	IDS、IPS、网闸、DDOS设备具有冗余机制，并验证有效性。	检查冗余机制并验证。			

5.6 管理要求

5.6.1 管理机构

表 5.6.1 管理机构评估内容及结果

序号	评估项	评估要求	评估方法及步骤	自评估结果	结果判定	整改措施
1.	人员配备	设立系统管理人员、网络管理人员、安全管理人员岗位，定义各个工作岗位的职责。	访谈管理人员并检查管理要求。			

2.		建立各审批事项的审批程序，按照审批程序执行审批过程。				
3.		专职安全管理人员不可兼任。				
4.	审核检查	安全管理人员定期进行安全检查，检查内容包括用户账号情况、系统漏洞情况、系统审计情况。				
5.	沟通机制	与供应商、业界专家、专业的安全公司、安全组织的合作与沟通机制。				

5.6.2 管理制度

表 5.6.2 管理制度评估内容及结果

序号	评估项	评估要求	评估方法及步骤	自评估结果	结果判定	整改措施
1.	管理制度	安全管理活动中的各类管理内容建立安全管理制度，以规范安全管理活动，约束人员的行为方式。	访谈管理人员并检查管理要求。			
2.	审核修订	对安全管理制度进行评审和修订，对存在不足或需要改进的安全管理制度进行修订。				

5.6.3 人员管理

表 5.6.3 人员管理评估内容及结果

序号	评估项	评估要求	评估方法及步骤	自评估结果	结果判定	整改措施
1.	人员管理	对管理人员、安全管理人员应签署保密协议。	访谈管理人员并检查管理要求。			
2.	安全培训	制定安全教育和培训计划，对信息安全基础知识、岗位操作规程等进行培训。				
3.	第三方访问管理	第三方人员应在访问或接入系统前与机构签署安全责任合同书或保密协议。				
4.		重要区域的访问，须提出书面申请，批准后由专人全程陪同或监督，并记录				

		备案。				

5.6.4 建设管理

表 5.6.4 建设管理评估内容及结果

序号	评估项	评估要求	评估方法及步骤	自评估结果	结果判定	整改措施
1.	建设管理	开发环境与实际运行环境物理分开。	检查系统环境。			
2.		应指定或授权专门的部门负责系统检测验收的管理，并按照管理制度的要求完成系统检测验收工作。	检查验收工作。			
3.		系统属性等资料报系统主管部门备案。	检查报备情况。			
4.		在应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动预案的条件、应急处理流程、系统恢复流程和事后教育和培训等内容。	访谈管理人员并检查应急预案。			
5.		对供应商进行有效管理，约定供应商（硬件和软件服务商）的 SLA。	访谈管理人员并检查供应商管理制度。			
6.		定期安全评估；提供定期评估的安全测评的报告，报告必须包含电子健康卡系统平台涉及的机房和网络设备的范围。 并应提供年度测评计划，要求对电子健康卡系统平台进行安全测评。	检查定期做安全评估情况，提供安全测评的报告。			

5.6.5 运维管理

5.6.5 运维管理评估内容及结果

序号	评估项	评估要求	评估方法及步骤	自评估结果	结果判定	整改措施
1.	运维管理	电子健康卡系统平台的管理和运维进行了培训，并有培训记录。	访谈管理人员并检查运维管理制度。			
2.		运维人员操作终端是专属运维终端，与互联网进行隔离的。				

3.		运维人员终端安装了防病毒软件。				
4.		运维人员拥有独立的账户，并总是使用自己的账户。				
5.		制定系统安全管理制度，对系统安全配置、系统帐户以及审计日志等方面作出规定。				
6.		专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析、处理工作。				
7.		定期进行网络系统漏洞扫描，对发现的网络系统安全漏洞进行及时的修补。				
8.		规定备份信息的备份方式（如增量备份或全备份等）、备份频度（如每日或每周等）、存储介质、保存期等。				
9.		规定备份信息的恢复目标，恢复时间进行定义。				
10.	带宽性能	互联网出口带宽应满足系统预期设计用户数的访问要求。	访谈管理人员并检查相应的带宽证明材料。			
11.		医疗机构专网带宽应满足系统预期设计用户数的访问要求。				
12.	稳定运行	系统在试运行期间能稳定运行，未出现服务中断情况。	检查系统日志和证明材料。			

附录B　电子健康卡管理信息系统自评估报告和承诺函模板

电子健康卡管理信息系统产品质量承诺函

我单位：XX（卡管运营单位），对YY（开发单位）开发的电子健康卡管理信息系统：xxxxxxx（卡管名称）VX.Y（版本号）、标识号：所提交的自评估报告进行评估审核后，认为其符合《电子健康卡建设与管理指南》和《电子健康卡技术规范 第2部分：管理信息系统》的相关要求，评估结果符合电子健康卡管理信息系统的质量要求。

我单位承诺对以上电子健康卡管理信息系统的产品质量、合规性和运行安全负责，确保电子健康卡管理信息系统的安全稳定运行。

承诺人签字：

单位名称：

（单位盖章）

日　　期：

电子健康卡管理信息系统
自评估报告

自评估单位信息	
自评估单位名称 （单位盖章）	
联　系　人	
联 系 电 话	
电 子 邮 件	

目 录

1 名词术语

表 1.1 名词术语

序号	名词术语	相关解释
（1）	电子健康卡	可通过二维码形式展现为电子健康卡，功能与实体居民健康卡相同。
（2）	电子健康卡管理信息系统	在电子健康卡注册用卡过程中，负责电子健康卡发卡数据的生产、使用和管理，采用电子账户对信息进行存储，并支持线下交互的技术应用。
（3）	主索引 ID	是标识居民健康卡用户唯一性的信息，通过主索引 ID 关联用户的实体居民健康卡、电子健康卡、医院就诊卡等不同类型账户。
（4）	电子健康卡 ID	电子健康卡管理系统用于标识电子健康卡账户唯一性的信息，电子健康卡 ID 由用户的证件类型和证件号码的密文组成。
（5）	电子健康卡二维码	电子健康卡通过二维码的形式予以展示，通过“面对面”方式进行交互使用。电子健康卡二维码包括静态二维码和动态二维码：静态二维码可通过移动 APP 呈现，也可印刷或粘贴于就诊卡等介质上，适用于挂号、问诊等非核心应用场景；动态二维码由 APP 呈现，在每次使用前生成，其生命周期根据应用安全的要求限定时间范围，适用于病历查询、结算交易等核心应用场景。
（6）	密码设备	密码设备是具有某种密码功能或能完成某种密码工作任务的设备的统称。
（7）	接入机构	接入使用电子健康卡管理信息系统，与平台提供接口存在交互逻辑的相关机构事业单位，包括但不限于医疗卫生机构、医保机构等。
（8）	接入 APP	接入电子健康卡管理信息系统，与平台接口存在交互逻辑的互联网移动应用软件。
（9）	电子健康卡 API 接口	是泛指远程连接到电子健康卡管理系统的 API 接口软件包，主要完成电子健康卡的注册、二维码申请、二维码验证等功能，接入 APP 通过 API 接口连接电子健康卡管理系统。
（10）	识读终端	识读二维码并与后台应用系统进行交互的终端，一般包括二维码的识读设备和终端机上的应用软件。

2 引用文档

2.1 评估标准

1) 《电子健康卡建设与管理指南》；
2) 《电子健康卡技术规范 第 2 部分：管理信息系统》；
3) 《电子健康卡技术规范 第 7 部分：跨域索引认证》。

2.2 参考资料

1) 卡管操作手册

3 评估资源

3.1 系统环境

电子健康卡管理信息系统拓扑图如下：

图 3.1 系统拓扑图

3.2 主要设备

主要设备包括：网络设备、服务器、密码机、识读终端
本次评估主要设备如下表：

表 3.2 主要设备列表

设备名称	规格型号	数量	备注

3.3 评估工具及设备

评估所使用测试工具/设备如下：

表 4.3 测试设备列表

设备名称	型号/版本号	生产商	用途

4 相关说明

4.1 评估结果判定

- 符合：首次评估结果既符合评估依据的要求。
- 不符合：评估过程中发现问题未整改或整改后评估结果为不符合评估依据的要求。
- 整改符合：评估过程中发现问题经整改后评估结果为符合评估依据的要求。
- 不适用：不具备规范中规定的条件必选项中的条件或不具备规范中的可选项功能。

4.2 评估结论判定

- 通过：所有必选项均符合或整改符合评估依据的要求则总结论为通过。
- 不通过：任何必选项评估不符合则总结论为不通过。

5 评估内容及结果

通过对电子健康卡管理信息系统的自评估，功能性共 40 项，全部符合/通过整改全部符合；性能效率共 3 项，全部符合/通过整改全部符合；信息安全性共测试 46 项，全部符合/通过整改全部符合；易用性共 3 项，全部符合/通过整改全部符合；可移植性共 1 项，全部符合/通过整改全部符合。具体评估内容及结果见以下内容：

5.1 功能性

表 5.1 功能性评估内容及结果

序号	评估项	评估点	评估要求	性质	自评估结果	结果判定
1.	电子健	账户信息	电子健康卡管理信息系	必选		

序号	评估项	评估点	评估要求	性质	自评估结果	结果判定
	康卡账户管理	管理	统应支持账户信息登记及管理			
2.		注册	电子健康卡管理信息系统应支持用户的注册	必选		
3.		查询	电子健康卡管理信息系统应支持用户的信息查询	必选		
4.		变更	电子健康卡管理信息系统应支持用户的信息变更	必选		
5.		绑卡	电子健康卡账户信息应支持与其它卡进行关联	必选		
6.		黑名单	电子健康卡管理信息系统应支持用户黑名单	必选		
7.		注销	电子健康卡管理信息系统应支持用户的注销	必选		
8.	机构管理	机构信息登记及管理	电子健康卡管理信息系统应支持机构信息登记及管理	必选		
9.		机构接入申请	电子健康卡管理信息系统应支持机构提交注册信息和接入申请	必选		
10.		机构接入授权	电子健康卡管理信息系统应支持机构接入授权	必选		
11.		机构信息查询	电子健康卡管理信息系统应支持机构信息查询	必选		
12.		机构信息变更	电子健康卡管理信息系统应支持机构信息变更	必选		
13.		机构信息批量导入	电子健康卡管理信息系统应支持机构信息批量导入	必选		
14.		黑名单	电子健康卡管理信息系统应支持机构黑名单	必选		
15.		机构退出	电子健康卡管理信息系	必选		

序号	评估项	评估点	评估要求	性质	自评估结果	结果判定
			统应支持中止机构合作关系			
16.	电子健康卡客户端应用软件管理	电子健康卡客户端应用软件信息登记及管理	电子健康卡管理信息系统应支持电子健康卡客户端应用软件信息登记及管理	必选		
17.		电子健康卡客户端应用软件接入申请	电子健康卡管理信息系统应支持电子健康卡客户端应用软件接入申请	必选		
18.		电子健康卡客户端应用软件接入授权	电子健康卡管理信息系统应支持电子健康卡客户端应用软件接入授权	必选		
19.		电子健康卡客户端应用软件信息查询	电子健康卡管理信息系统应支持电子健康卡客户端应用软件信息查询	必选		
20.		电子健康卡客户端应用软件信息变更	电子健康卡管理信息系统应支持电子健康卡客户端应用软件信息变更	必选		
21.		电子健康卡客户端应用软件停用/启用	电子健康卡管理信息系统应支持电子健康卡客户端应用软件停用/启用	必选		
22.	识读终端管理	识读终端信息登记及管理	电子健康卡管理信息系统应支持识读终端信息登记及管理	必选		
23.		识读终端接入申请	电子健康卡管理信息系统应支持机构提交的识读终端注册申请	必选		
24.		识读终端接入授权	电子健康卡管理信息系统应支持识读终端接入	必选		

序号	评估项	评估点	评估要求	性质	自评估结果	结果判定
			授权			
25.		识读终端信息查询	电子健康卡管理信息系统应支持识读终端信息查询	必选		
26.		识读终端退出	电子健康卡管理信息系统应支持中止识读终端的接入	必选		
27.	二维码管理	二维码申请	电子健康卡管理信息系统应支持二维码申请接口	必选		
28.		二维码本地验证	电子健康卡管理信息系统应支持二维码本地验证	必选		
29.		二维码跨域验证	电子健康卡管理信息系统应支持二维码跨域验证	必选		
30.		二维码使用记录	电子健康卡管理信息系统应支持二维码使用记录查询和分析	必选		
31.	密码模块管理	密码模块信息登记	电子健康卡管理信息系统应支持密码模块信息登记	必选		
32.		密码模块接口	密码模块接口应符合技术规范的要求，且使用正常	必选		
33.	外部接口	用卡监测系统接口	电子健康卡管理信息系统应支持用卡监测系统接口	必选		
34.	数据审计	用卡数据统计	电子健康卡管理信息系统应能够对用卡数据进行实时监测和统计	必选		
35.		发卡数据统计	电子健康卡管理信息系统应能够对发卡数据进行实时监测和统计	必选		

序号	评估项	评估点	评估要求	性质	自评估结果	结果判定
36.		用卡数据分析	电子健康卡管理信息系统应能够提供用卡数据反查接口，通过该接口，实现用卡数据反查	必选		
37.		发卡数据分析	电子健康卡管理信息系统应能够提供 f 卡数据反查接口，通过该接口，实现发卡数据反查	必选		

5.2 性能效率

表 5. 2 性能效率评估内容及结果

序号	评估项	评估要求	性质	自评估结果	结果判定
1.	用户注册支持多用户并发操作	运行于单台服务器时应不低于 1000 并发用户，响应时间不高于 3 秒，事务成功率不低于 99%，应用及数据库服务器 CPU、内存资源利用率不高于 85%	必选		
		截图			
2.	二维码生成支持多用户并发操作	运行于单台服务器时应不低于 1000 并发用户，响应时间不高于 3 秒，事务成功率不低于 99%，，应用及数据库服务器 CPU、内存资源利用率不高于 85%	必选		
3.	二维码验证支持多用户并发操作	运行于单台服务器时应不低于 1000 并发用户，响应时间不高于 3 秒，事务成功率不低于 99%，应用及数据库服务器 CPU、内存资源利用率不高于 85%	必选		

5.3 信息安全性

表 5.3 信息安全性评估内容及结果

序号	评估项	评估点	评估要求	性质	自评估结果	结果判定
1.	身份鉴别	系统与普通用户设置	业务系统、管理信息系统应提供专用的登录控制模块对登录用户进行身份标识和鉴别。	必选		
2.			应提供系统管理员和普通用户的设置功能。	必选		
3.		身份标识唯一性	应提供用户身份标识唯一性和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用。	必选		
4.			应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。	必选		
5.		登录访问安全策略	应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别。	推荐		
6.		口令有效期限制	业务系统、管理信息系统应限制口令的有效期限，并进行提醒。	必选		
7.		非法访问警示和记录	业务系统、管理信息系统应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。	推荐		
8.			业务系统、管理信息系统应对登录成功、失败进行日志记录。	推荐		
9.		限制认证会话	业务系统、管理信息系统应对客户端认证会话时间进	必选		

序号	评估项	评估点	评估要求	性质	自评估结果	结果判定
		时间	行限制。			
10.		及时清除鉴别信息	业务系统、管理信息系统会话结束后应及时清除客户端鉴别信息。	必选		
11.	访问控制	访问权限设置	应提供访问控制功能。	必选		
12.			控制粒度应达到文件、数据库级。	必选		
13.			访问控制策略的授权主体。	必选		
14.			如设置默认用户，其权限有应被严格限制。	必选		
15.			各用户权限划分应依据最小权限原则，相互之间应存在制约关系。	必选		
16.		自主访问控制范围	访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作。	推荐		
17.		业务操作日志	应提供业务操作审计功能。	必选		
18.		关键数据操作控制	应严格控制用户对关键数据的操作。关键数据如：敏感数据、重要业务数据、系统管理数据等。	必选		
19.		异常中断维护	应提供用户访问中断的保护措施，应保证数据不丢失	必选		
20.	安全审计	对象操作审计	应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计。	必选		
21.		日志信息	应具备安全审计功能。	必选		
22.			审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等。	必选		

序号	评估项	评估点	评估要求	性质	自评估结果	结果判定
23.		日志权限和保护	应保证无法单独中断审计进程。	必选		
24.			无法删除、修改或覆盖审计记录。	必选		
25.		系统信息查询和分析	应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。	推荐		
26.	资源控制	会话控制	当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话。	必选		
27.			应能够对单个账户的多重并发会话进行限制。	必选		
28.	应用容错	数据有效性校验	应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。	必选		
29.		故障机制	发生故障后，系统应能够及时恢复，系统应能够记录异常信息。	必选		
30.	报文完整性	通信报文有效性	通信报文应采用密码技术保证通讯过程中交易数据的完整性。	必选		
31.	报文保密性	报文或会话加密	在通讯时采用安全通道或对报文中敏感信息进行加密。	必选		
32.		敏感信息显示	应对系统中的敏感信息（如身份证、手机号、金融账号等）进行脱敏显示	必选		
33.	存储安全性	数据加密存储	在存储时采用安全机制对数据中敏感信息以及存储敏感信息的日志进行加密	必选		
34.		数据存	应采用校验技术或者密码	必选		

序号	评估项	评估点	评估要求	性质	自评估结果	结果判定
		储完整性	技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要个人信息等。			
35.	WEB 页面安全	登录防穷举	业务系统、管理信息系统应提供登录防穷举的措施，如图片验证码等。	必选		
36.			登录失败后图形验证码应能自动更换。	必选		
37.			图形验证码应该具备一定的复杂度，防止能够轻易地被自动化工具识别。	必选		
38.		网站页面注入防范	业务系统、管理信息系统应无 SQL 注入、Path 注入和 LDAP 注入等漏洞。	必选		
39.		网站页面跨站脚本攻击防范	业务系统、管理信息系统应无跨站脚本漏洞。	必选		
40.		网站页面源代码暴露防范	业务系统、管理信息系统应无源代码暴露漏洞。	必选		
41.		网站页面黑客挂马防范	应采取防范网站页面黑客挂马的机制和措施。	必选		
42.	剩余信息保护	剩余信息保护	应保证存有剩余信息的存储空间被释放或重新分配给其他用户前得到完全清除。	必选		
43.	数据备	数据备份和恢	应提供本地数据备份与恢复功能	必选		

序号	评估项	评估点	评估要求	性质	自评估结果	结果判定
44.	份和恢复	复	应提供重要数据处理系统的热冗余，保证系统的高可用性	必选		
45.	个人信息保护	个人信息保护	应仅采集和保存业务必需的用户个人信息	必选		
46.			应禁止未授权访问和非法使用用户个人信息	必选		

5.4 易用性

表 5.4 易用性评估内容及结果

序号	评估项	评估点	评估要求	性质	自评估结果	结果判定
1.	易用性	易理解性	有关系统执行的问题、消息和结果应是易理解的	必选		
2.			源自系统的消息应设计成使最终用户易理解的形式	必选		
3.			屏幕输入格式、报表和其他输出对用户来说应是清晰且易理解的	必选		
4.		易学性	借助用户界面、帮助功能、用户文档提供的手段，最终用户能够学习如何使用某一功能	必选		
5.		易操作性	用户界面应显示正常，界面风格应一致，输入输出正	必选		
6.			具有严重后果的功能执行应是可逆的，或者系统应给出该后果的明显警告，并且在该操作执行前要求确认	必选		

5.5 可移植性

表 5.4 可移植性评估内容及结果

序号	评估项	评估点	评估要求	性质	自评估结果	结果判定
1.	可移植性	支持跨平台部署	系统应支持跨平台部署，支持 Linux、Windows、国产操作系统	必选		

附录C　电子健康卡客户端应用软件（APP）接入自评估报告和承诺函模板

电子健康卡客户端应用软件接入承诺函

我单位：XX（卡管运营单位），对YY（开发单位）开发的客户端应用软件xxxxxxx（应用名称）VX.Y（版本号），Android/iOS版本，登记编号：所提交的自评估报告进行评估审核后，认为其符合《电子健康卡建设与管理指南》和《电子健康卡技术规范 第5部分：客户端应用软件》的相关要求，评估结果符合接入要求。

我单位承诺对以上电子健康卡客户端应用软件的产品质量、合规性和运行安全负责，确保电子健康卡客户端应用软件的安全稳定运行。

承诺人签字：

单位名称：

（单位盖章）

日　　期：

电子健康卡客户端应用软件
接入自评估报告

自评估单位信息	
自评估单位名称 （单位盖章）	
联　系　人	
联 系 电 话	
电 子 邮 件	

目录

1 名词术语

表 1.1 名词术语

序号	名词术语	相关解释
（2）	电子健康卡	可通过二维码形式展现为电子健康卡，功能与实体居民健康卡相同。
	电子健康卡管理信息系统	在电子健康卡注册用卡过程中，负责电子健康卡发卡数据的生产、使用和管理，采用电子账户对信息进行存储，并支持线下交互的技术应用。
	主索引 ID	是标识居民健康卡用户唯一性的信息，通过主索引 ID 关联用户的实体居民健康卡、电子健康卡、医院就诊卡等不同类型账户。
	电子健康卡 ID	电子健康卡管理系统用于标识电子健康卡账户唯一性的信息，电子健康卡 ID 由用户的证件类型和证件号码的密文组成。
	电子健康卡二维码	电子健康卡通过二维码的形式予以展示，通过“面对面”方式进行交互使用。电子健康卡二维码包括静态二维码和动态二维码：静态二维码可通过移动 APP 呈现，也可印刷或粘贴于就诊卡等介质上，适用于挂号、问诊等非核心应用场景；动态二维码由 APP 呈现，在每次使用前生成，其生命周期根据应用安全的要求限定时间范围，适用于病历查询、结算交易等核心应用场景。
	密码设备	密码设备是具有某种密码功能或能完成某种密码工作任务的设备的统称。
	接入机构	接入使用电子健康卡管理信息系统，与平台提供接口存在交互逻辑的相关机构事业单位，包括但不限于医疗卫生机构、医保机构等。
	接入 APP	接入电子健康卡管理信息系统，与平台接口存在交互逻辑的互联网移动应用软件。
	电子健康卡 API 接口	是泛指远程连接到电子健康卡管理系统的 API 接口，主要完成电子健康卡的注册、二维码申请、二维码验证等功能，接入 APP 通过 API 接口连接电子健康卡管理系统。
	识读终端	识读二维码并与后台应用系统进行交互的终端，一般包括二维码的识读设备和终端机上的应用软件。

2 引用文档

2.1评估标准

3) 《电子健康卡建设与管理指南 V3.1（需要按照最新发布指南）》；
4) 《电子健康卡技术规范 第 5 部分：客户端应用软件（需要按照最新发布技术规范）》。

2.2参考资料

1) 例：客户端应用软件开发文档

3 评估资源

3.1系统环境

系统拓扑图如下。

图 3.1 系统拓扑图

3.2主要设备

主要设备包括：客户端应用软件服务器、卡管系统服务器、密码机等
本次评估主要设备如下表：

表 3.2 主要设备列表

设备名称	规格型号	数量	备注

3.3评估工具及设备

评估所使用工具/设备如下：

表 3.3 评估设备列表

软件/设备名称	版本号/型号	生产商	用途
评估设备应包括客户端应用软件安全评估的相应软件工具、设备及手机			

4 相关说明

4.1评估结果判定

- 符合：评估结果既符合评估依据的要求。
- 不符合：评估过程中发现问题未整改或整改后评估结果为不符合评估依据的要求。

- 整改符合：评估过程中发现问题经整改后评估结果为符合评估依据的要求。

4.2评估结论判定

- 通过：所有必选项均符合或整改符合评估依据的要求则总结论为通过。
- 不通过：任何必选项评估不符合则总结论为不通过。

5 评估内容及结果

说明：接入评估所有评估项为必选项。

客户端应用软件接入评估功能性共 11 项，通过整改全部符合/全部符合；信息安全性共 19 项，符合 xx 项，不符合 xx 项；接口共 5 项，通过整改全部符合；UI 共 4 项，全部符合；稳定性共 3 项，通过整改全部符合；性能效率共 4 项，符合 xx 项，不符合 xx 项；具体评估内容及结果见下表。

5.7 功能性

表 5.1 功能评估内容及结果

序号	评估项	评估要求	评估结果	结果判定	整改措施
14.	实名制注册	客户端应用软件应具备用户实名制注册功能及相应的操作流程。	应描述评估结果 例：具备用户实名制注册功能及相应操作流程	**符合/整改符合/不符合**	
15.	用户身份认证	客户端应用软件应提供多种用户身份认证功能，如静态口令身份验证功能、动态口令身份验证功能、生物识别身份验证功能、基于密钥身份验证功能等。	例：提供用户名+静态口令身份验证和手机号+验证码动态口令身份验证进行身份认证	**符合/整改符合/不符合**	
16.	就诊卡账户绑定	客户端应用软件应具备就诊卡账户绑定功能（如无此功能，则为不适用）。			
17.	就诊信息查询	客户端应用软件应具备就诊信息查询功能（如无此功能，则为不适用）。			
18.	二维码申请	客户端应用软件应具备二维码申请功能。			

序号	评估项	评估要求	评估结果	结果判定	整改措施
19.	二维码接收	客户端应用软件应具备二维码接收功能。			
20.	二维码生成	客户端应用软件应具备二维码生成功能。			
21.	交互结果通知	客户端应用软件应具备交互结果通知功能。			
22.	用户解绑	客户端应用软件应具备用户解绑功能。	需提供相应截图证明		
23.	登记注册备案	客户端应用软件应在卡管系统中登记注册，并获取备案编号。	需提供相应截图证明		
24.	备案编号配置	验证 1. Android 版本是否将备案编号保存在 AndroidManifest.xml 中 2.iOS 版本是否将备案编号保存在 info.plist 中。 3.备案编号字段名称是否为“EHCI_KEY”。	需提供相应截图证明		

5.8 信息安全性

5.8.1 自身安全性

表 5.2.1 信息安全性评估内容及结果

序号	评估项	评估要求	自评估结果	结果判定	整改措施
9.	软件更新	验证通过客户端应用软件的更新流程。 验证软件更新包的合法性。	应使用测试工具进行验证 需提供相应截图证明		
10.	客户端签名	检查开发文档中关于客户端应用软件签名的安全要求和实现机制。 防止重新打包后的软件可以正常使用。	需提供相应截图证明		
11.	应用软件的自检	应用软件启动时应执行自检程序及检查软件运行环境 。	需提供相应截图证明		
12.	合法性认证和风险控制	1. 检查开发文档中关于安全协议层的安全认			

序号	评估项	评估要求	自评估结果	结果判定	整改措施
		证要求。 增强要求： 2. 查看服务端对客户端的身份认证方式，包括提供对手机号码绑定或客户端标识符绑定等认证方式，并验证其有效性。 3. 查看客户端对服务器端的身份认证方式，包括提供服务器证书，并验证其有效性。			

5.8.2 用户安全鉴别

表 5. 2. 2 用户安全鉴别评估内容及结果

序号	评估项	评估要求	自评估结果	结果判定	整改措施
1.	用户标识	1. 当进入客户端时，应先进行标识（如建立账号），没有进行标识的用户不能进入系统。 2. 新建立一个账号，其用户标识为已有用户的标识（如用户名），则新建失败。	需提供相应截图证明		
2.	手势密码	1. 开发文档中应提供客户端软件手势密码的点长度要求。 2. 在添加手势密码时，添加短于或长于要求的长度，应给出相应提示。 3. 在应用软件启动手势密码时，应检查手势密码的界面安全。	需提供相应截图证明		
3.	生物标志密码	1. 开发文档中应提供客户端软件生物标志（指纹、虹膜等）密码	需提供相应截图证明		

序号	评估项	评估要求	自评估结果	结果判定	整改措施
		的要求。 2. 在应用软件启动生物标志密码时，应检查生物标志密码的界面安全。			
4.	重验证机制	1. 在执行密码重置前，应对用户身份进行重新验证。 2. 开发文档中客户端软件应提供会话超时重鉴别功能，并确认其超时阈值。 3. 空闲操作达到设置阈值，应提供重验证功能。	需提供相应截图证明		
5.	验证信息（密码）保护	1. 检查确认客户端软件关于用户身份认证信息的存储情况。 2. 确认数据的加解密方式、加密密钥长度及密钥管理方式。 3. 尝试截获远程敏感数据的传输，其应采取安全加密措施。 4. 检查口令的长度、复杂度及更改周期等。 5. 开发文档中应提供验证码可重复使用的次数限制。 6. 在客户端验证码可重复使用的次数限制。	需提供相应截图证明		
6.	失败的验证	查看客户端是否限制无效验证次数。	需提供相应截图证明		
7.	短信验证码	1. 用户预留手机号码信息应保存于服务端数	需提供相应截图证明		

序号	评估项	评估要求	自评估结果	结果判定	整改措施
		据库中。 2. 检查短信验证码的长度及随机性，在有效时间内，短信验证码应仅可使用一次，有效时间不应超过 10 分钟。 3. 应限制单个用户一定时间内的使用频次。			

5.8.3 数据安全

表 5. 2. 3 数据安全评估内容及结果

序号	评估项	评估要求	自评估结果	结果判定	整改措施
1.	数据的输入	1. 检查开发文档中关于敏感信息显示的规定。 2. 用户通过客户端软件登录时输入的登录密码不应以明文的方式显示。 3. 用户通过客户端软件进行支付操作时，输入的支付密码不应以明文方式显示。 4. 若客户端软件中存在其它需要用户输入的敏感数据，则不应以明文的方式显示。	需提供相应截图证明		
2.	数据的传输	1. 检查开发文档中关于安全协议层的安全认证要求。 2. 应采取有效措施以确保敏感数据的保密性。 3. 尝试截获远程敏感数据的传输，其应采取	需提供相应截图证明		

序号	评估项	评估要求	自评估结果	结果判定	整改措施
		安全加密措施。 增强要求： 4. 查看服务端对客户端的身份认证方式，包括提供对手机号码绑定或客户端标识符绑定等认证方式，并验证其有效性。 5. 查看客户端对服务器端的身份认证方式，包括提供服务器证书，并验证其有效性。			
3.	数据的加密	确认数据的加解密方式、加密密钥长度及密钥管理方式。	需提供相应截图证明		
4.	数据的存储	1. 检查开发文档中关于客户端软件敏感数据的保留情况，应对保留的空间和时间进行限制，并明确保留的位置。 2. 检查确认客户端软件关于敏感数据的存储情况。	需提供相应截图证明		
5.	残余信息保护	1. 检查开发文档中客户端软件防止内存中残留敏感信息的措施。 2. 在客户端应用软件上输入敏感信息并完成相应功能的操作后，敏感信息不应有残留。	需提供相应截图证明		

5.8.4 接入安全

表 5. 2. 4 接入安全评估内容及结果

序号	评估项	评估要求	自评估结果	结果判定	整改措施
1.	授权接入	检查客户端应用软件是	需提供相应截图证		

序号	评估项	评估要求	自评估结果	结果判定	整改措施
		否按照电子健康卡管理信息系统接入层认证方案进行安全接入。	明		

5.8.5 二维码安全

表 5. 2. 5 二维码安全评估内容及结果

序号	评估项	评估要求	自评估结果	结果判定	整改措施
1.	二维码申请	客户端应用软件从后台服务器获取条码时，后台应对用户身份进行身份验证。	需提供相应截图证明		
2.	二维码显示	1. 二维码不包含敏感信息，应采用加密技术对条码关键信息进行保护。 2. 二维码显示界面应进行防截屏保护。 3. 如有支付功能时，验证二维码是否动态定时刷新，刷新时间间隔不超过 60 秒。	需提供相应截图证明		

5.9 接口

表 5. 3 接口评估内容及结果

序号	评估项	评估要求	自评估结果	结果判定	整改措施
1.	与电子健康卡管理信息系统接口	客户端应用软件或第三方服务号应正确实现与系统的接口交互，且具备异常处理能力。			
2.	接口数据完整性	客户端应用软件或第三方服务号应提供保障接口数据的完整性和异常检查能力。			
3.	接口报文功	客户端应用软件或第三			

序号	评估项	评估要求	自评估结果	结果判定	整改措施
	能性	方服务号应正确实现报文交互和解析功能。			
4.	不同网络环境适配	客户端应用软件或第三方服务号应具备在不同网络状态下的正常处理能力。			
5.	授权接入认证	客户端应用软件或第三方服务号应具备授权接入认证能力。	需提供相应截图证明		

5.10 UI

表 5.4 UI 评估内容及结果

序号	评估项	评估要求	自评估结果	结果判定	整改措施
1.	居民健康卡标识展示	客户端应用软件或第三方服务号应将二维码与居民健康卡标识（LOGO）相结合，展现居民健康卡品牌性。	需提供相应截图证明		
2.	备案编号标识展示	客户端应用软件或第三方服务号应在电子健康卡展示页面的显著位置向用户提供该客户端备案编号的标识，备案编号应与配置文件中保持一致。	需提供相应截图证明		
3.	界面 UI 布局、功能	客户端应用软件或第三方服务号 UI 界面应在主流手机屏幕上正常展示及实现正确的用户交互操作。			
4.	展示完整性	客户端应用软件或第三方服务号应在主流手机屏幕上完整展示信息。			

5.11 稳定性

表 5.5 稳定性评估内容及结果

序号	评估项	评估要求	自评估结果	结果判定	整改措施
1.	启动可靠性	客户端应用软件应在主流手机上正确启动。			
2.	操作流畅性	客户端应用软件应在主流手机上实现与用户的流程交互，无严重卡顿、无响应现象。			
3.	健壮性	客户端应用软件应正确处理各类异常，在大量多次操作下，无强制关闭、异常崩溃、应用无法关闭、弹窗无法关闭等严重问题。			

5.12 性能效率

表 5.6 性能效率评估内容及结果

序号	评估项	评估要求	自评估结果	结果判定	整改措施
1.	启动耗时	查看应用软件在典型配置的手机上的启动耗时不超过 5 秒。	需提供相应工具截图证明		
2.	CPU 占用率	查看应用软件运行时的 CPU 占用率，均值应低于 30%。	需提供相应工具截图证明		
3.	内存占用率	查看应用软件运行时的内存占用率不超过运行内存的 30%。	需提供相应工具截图证明		
4.	关键操作耗时	应用软件的生成二维码的整体耗时应不超过 3 秒。	需提供相应工具截图证明		

附录D　电子健康卡客户端应用软件（第三方服务号）接入自评估报告和承诺函模板

电子健康卡客户端应用软件接入承诺函

我单位：XX（卡管运营单位），对YY（开发单位）开发的客户端应用软件xxxxxxx（应用名称）VX.Y（版本号），微信公众号/其他（运行平台），登记编号：所提交的自评估报告进行评估审核后，认为其符合《电子健康卡建设与管理指南》和《电子健康卡技术规范 第5部分：客户端应用软件》的相关要求，评估结果符合接入要求。

我单位承诺对以上电子健康卡客户端应用软件的产品质量、合规性和运行安全负责，确保电子健康卡客户端应用软件的安全稳定运行。

承诺人签字：

单位名称：

（单位盖章）

日　　期：

电子健康卡客户端应用软件
接入自评估报告

自评估单位信息	
自评估单位名称 （单位盖章）	
联　系　人	
联 系 电 话	
电 子 邮 件	

目录

1 名词术语

表 1.1 名词术语

序号	名词术语	相关解释
（3）	电子健康卡	可通过二维码形式展现为电子健康卡，功能与实体居民健康卡相同。
	电子健康卡管理信息系统	在电子健康卡注册用卡过程中，负责电子健康卡发卡数据的生产、使用和管理，采用电子账户对信息进行存储，并支持线下交互的技术应用。
	主索引 ID	是标识居民健康卡用户唯一性的信息，通过主索引 ID 关联用户的实体居民健康卡、电子健康卡、医院就诊卡等不同类型账户。
	电子健康卡 ID	电子健康卡管理系统用于标识电子健康卡账户唯一性的信息，电子健康卡 ID 由用户的证件类型和证件号码的密文组成。
	电子健康卡二维码	电子健康卡通过二维码的形式予以展示，通过“面对面”方式进行交互使用。电子健康卡二维码包括静态二维码和动态二维码：静态二维码可通过移动 APP 呈现，也可印刷或粘贴于就诊卡等介质上，适用于挂号、问诊等非核心应用场景；动态二维码由 APP 呈现，在每次使用前生成，其生命周期根据应用安全的要求限定时间范围，适用于病历查询、结算交易等核心应用场景。
	密码设备	密码设备是具有某种密码功能或能完成某种密码工作任务的设备的统称。
	接入机构	接入使用电子健康卡管理信息系统，与平台提供接口存在交互逻辑的相关机构事业单位，包括但不限于医疗卫生机构、医保机构等。
	接入 APP	接入电子健康卡管理信息系统，与平台接口存在交互逻辑的互联网移动应用软件。
	电子健康卡 API 接口	是泛指远程连接到电子健康卡管理系统的 API 接口，主要完成电子健康卡的注册、二维码申请、二维码验证等功能，接入 APP 通过 API 接口连接电子健康卡管理系统。
	识读终端	识读二维码并与后台应用系统进行交互的终端，一般包括二维码的识读设备和终端机上的应用软件。

2 引用文档

2.1评估标准

5) 《电子健康卡建设与管理指南 V3.1（需要按照最新发布指南）》；
6) 《电子健康卡技术规范 第 5 部分：（需要按照最新发布技术规范）》。

2.2参考资料

2) 例：客户端应用软件开发文档

3 评估资源

3.1系统环境

系统拓扑图如下。

图 4.1 系统拓扑图

3.2主要设备

主要设备包括：客户端应用软件服务器、卡管系统服务器、密码机
本次评估主要设备如下表：

表 3.2 主要设备列表

设备名称	规格型号	数量	备注

3.3评估工具及设备

评估所使用工具/设备如下：

表 3.3 评估设备列表

软件/设备名称	版本号/型号	生产商	用途
评估设备应包括客户端应用软件安全评估的相应软件工具、设备及手机			

4 相关说明

4.1评估结果判定

- 符合：评估结果既符合评估依据的要求。
- 不符合：评估过程中发现问题未整改或整改后评估结果为不符合评估依

据的要求。

- 整改符合：评估过程中发现问题经整改后评估结果为符合评估依据的要求。

4.2评估结论判定

- 通过：所有必选项均符合或整改符合评估依据的要求则总结论为通过。
- 不通过：任何必选项评估不符合则总结论为不通过。

5 评估内容及结果

说明：接入评估所有评估项为必选项。

客户端应用软件接入评估功能性共 9 项，通过整改全部符合/全部符合；信息安全性共 13 项，符合 xx 项，不符合 xx 项；接口共 5 项，通过整改全部符合；UI 共 4 项，全部符合；稳定性共 2 项，通过整改全部符合；性能效率共 1 项，符合 xx 项，不符合 xx 项；具体评估内容及结果见下表。

5.13 功能性

表 5.1 功能性评估内容及结果

序号	评估项	评估要求	评估结果	结果判定	整改措施
25.	电子健康卡二维码申请功能	验证电子健康卡客户端应用软件是否具备二维码申请功能，申请信息应包含姓名、证件类型、经验证的证件号码、经验证的手机号等必填项，及就诊人类型、医保类型、所在区域、地址等可选项	应描述评估结果	**符合/整改符合/不符合**	
26.	电子健康卡二维码接收功能	验证电子健康卡客户端应用软件是否具备二维码接收功能		**符合/整改符合/不符合**	
27.	电子健康卡二维码显示功能	验证电子健康卡客户端应用软件是否具备二维码显示功能			
28.	用户身份认证功能	验证电子健康卡客户端应用软件是否提供多种用户身份认证功能，如静态口令身份验证功			

序号	评估项	评估要求	评估结果	结果判定	整改措施
		能、动态口令身份验证功能、生物识别身份验证功能、基于密钥身份认证功能等。			
29.	就诊卡账户绑定功能	验证电子健康卡客户端应用软件是否具备就诊卡账户绑定功能（如无此功能，则为不适用）。			
30.	就诊信息查询	验证电子健康卡客户端应用软件是否具备就诊信息查询功能（如无此功能，则为不适用）。			
31.	电子健康卡解绑功能	验证电子健康卡客户端应用软件是否具备和电子健康卡管理信息系统解绑的功能。	需提供相应截图证明		
32.	登记注册备案	电子健康卡第三方服务号应在卡管系统中登记注册,并获取备案编号。	需提供相应截图证明		
33.	备案编号配置	验证： 1. 电子健康卡第三方服务号是否在域名下自建备案编号文件，名称为“EHCI_KEY”（无后缀名），备案号采用utf-8编码保存在该文件中。 2. 如果一个服务号有多个备案号，应在该文件中同时保存多个备案号，用英文逗号隔开。	需提供相应截图证明		

5.14 信息安全性

5.14.1 页面安全性

表 5.2.1 页面安全评估内容及结果

序号	评估项	评估要求	自评估结果	结果判定	整改措施
13.	访问方式	客户端应用软件通过HTTPS 方式传输，使用	使用测试工具进行安全性评估		

序号	评估项	评估要求	自评估结果	结果判定	整改措施
		国家认可的加密方式，推荐使用国密算法	需提供相应截图证明		
14.	页面注入防范	检查页面不存在 SQL 注入、LDAP 注入等漏洞	需提供相应工具截图证明		
15.	页面跨站脚本攻击	通过 Web 扫描软件及手工测试，检查页面是否存在 XSS 跨站脚本等漏洞	需提供相应工具截图证明		
16.	页面源代码暴露	通过 Web 扫描软件及手工测试，检查页面是否存在源代码信息泄露等	需提供相应工具截图证明		
17.	页面黑客挂马	通过 Web 扫描软件及手工测试，检查页面是否被黑客挂马或是否有被挂马等风险	需提供相应工具截图证明		

5.14.2 数据安全

表 5. 2. 3 数据安全评估内容及结果

序号	评估项	评估要求	自评估结果	结果判定	整改措施
6.	数据的输入	1. 检查开发文档中关于敏感信息显示的规定。 2. 查看用户通过客户端应用软件登录时输入的登录密码是否以明文的方式显示。 3. 查看用户通过客户端应用软件存在其它需要用户输入的敏感数据，则查看是否以明文的方式显示。	需提供相应截图证明		
7.	数据的传输	1. 检查开发文档中关于安全协议层的安全认证要求。 2. 查看是否采取了有效措施以确保敏感	需提供相应截图证明		

序号	评估项	评估要求	自评估结果	结果判定	整改措施
		数据的保密性。 3. 尝试截获远程敏感数据的传输，验证其是否采取安全加密措施。			
8.	数据的加密	1. 确认数据的加解密方式、加密密钥长度及密钥管理方式。	需提供相应截图证明		
9.	数据的存储	1. 检查开发文档中关于客户端应用软件敏感数据的保留情况，保留的空间和时间是否进行限制，并明确保留的位置。 2. 检查确认电子健康卡客户端应用软件关于敏感数据的存储情况。	需提供相应截图证明		
10.	残余信息保护	1. 检查开发文档中电子健康卡客户端应用软件防止内存中残留敏感信息的措施。 2. 在客户端应用软件上输入敏感信息并完成相应功能的操作后，测试验证敏感信息的残留情况。	需提供相应截图证明		

5.14.3 接入安全

表 5. 2. 4 接入安全评估内容及结果

序号	评估项	评估要求	自评估结果	结果判定	整改措施

序号	评估项	评估要求	自评估结果	结果判定	整改措施
2.	授权接入	检查客户端应用软件是否按照电子健康卡管理信息系统接入层认证方案进行安全接入。	需提供相应截图证明		

5.14.4 二维码安全

表 5. 2. 5 二维码安全评估内容及结果

序号	评估项	评估要求	自评估结果	结果判定	整改措施
3.	二维码申请	检查客户端应用软件从后台服务器获取条码时，后台是否对用户身份进行身份验证。	需提供相应截图证明		
4.	二维码显示	1、查看二维码是否符合技术指引中对二维码的要求。 2、验证二维码是否动态定时刷新。	需提供相应截图证明		

5.15 接口

表 5. 3 接口评估内容及结果

序号	评估项	评估要求	自评估结果	结果判定	整改措施
6.	与电子健康卡管理信息系统接口	客户端应用软件应正确实现与系统的接口交互，且具备异常处理能力。			
7.	接口数据完整性	客户端应用软件应提供保障接口数据的完整性和异常检查能力。			
8.	接口报文功能性	客户端应用软件应正确实现报文交互和解析功能。			
9.	不同网络环境适配	客户端应用软件应具备在不同网络状态下的正常处理能力。			
10.	授权接入认证	客户端应用软件或第三	需提供相应截图证明		

序号	评估项	评估要求	自评估结果	结果判定	整改措施
		方服务号应具备授权接入认证能力。			

5.16 UI

表 5.4 UI 评估内容及结果

序号	评估项	评估要求	自评估结果	结果判定	整改措施
5.	居民健康卡标识展示	客户端应用软件应将二维码与居民健康卡标识（LOGO）相结合，展现居民健康卡品牌性。	需提供相应截图证明		
6.	备案编号标识展示	客户端应用软件或第三方服务号应在电子健康卡展示页面的显著位置向用户提供该客户端备案编号的标识，备案编号应与配置文件中保持一致。	需提供相应截图证明		
7.	界面 UI 布局、功能	客户端应用软件 UI 界面应在主流手机屏幕上正常展示及实现正确的用户交互操作。			
8.	展示完整性	客户端应用软件应在主流手机屏幕上完整展示信息。			

5.17 稳定性

表 5.5 稳定性评估内容及结果

序号	评估项	评估要求	自评估结果	结果判定	整改措施
4.	操作流畅性	验证电子健康卡客户端应用软件是否在主流手机上可以实现与用户的流程交互，无严重卡顿、无响应现象。			
5.	健壮性	验证电子健康卡客户端			

序号	评估项	评估要求	自评估结果	结果判定	整改措施
		应用软件是否正确处理各类异常，在大量多次操作下，无强制关闭、异常崩溃、应用无法关闭、弹窗无法关闭等严重问题。			

5.18 性能效率

表 5.6 性能效率评估内容及结果

序号	评估项	评估要求	自评估结果	结果判定	整改措施
5.	关键操作耗时	验证电子健康卡客户端应用软件的生成二维码的整体耗时不超过 3 秒。	需提供相应工具截图证明		

附录E　固定式条码扫描设备自评估报告模板

固定式条码扫描设备检测现场自评估报告

自评估单位信息	
自评估单位名称 （单位盖章）	
联　系　人	
联 系 电 话	
电 子 邮 件	

自 评 报 告

产品名称		规格型号	
生产单位		样品数量	3 台
生产单位 地 址		测试地点	
生产日期		抽样数量	/
检验日期		抽样基数	/
检验依据	GB/T 17618-2015《信息技术设备抗扰度限值和测量方法》 GB/T 9254-2008 《信息技术设备的无线电骚扰限值和测量方法》 《电子健康卡技术规范 第 4 部分：识读终端》		
检验项目	外观和结构、性能及功能检查、电源适应能力、安全性要求、环境适应性试验、电磁兼容性检验		
检 验 结 论	根据检验依据和判定（参考）依据栏中所列标准及要求，对送检样品进行了外观和结构、性能及功能检查、电源适应能力、安全性要求、环境适应性试验、电磁兼容性检验项目检验（试验），其中安全性要求(接地导体及其连接的电阻、接触电流和保护导体电流、抗电强度)不适用，检验项目结果详见后。		
备注	/		

批准： 审核： 主检：

本次检验用主要仪器设备			
序号	仪器设备名称	仪器编号	计量有效期
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
此处空白			

样品分配情况		
样品编号	样品出厂编号	检验项目
001	/	外观和结构、性能及功能检查、电源适应能力、安全性要求
002	/	环境适应性试验
003	/	电磁兼容性检验
注：下文中“样品编号”仅保留后三位序列号，与此处后三位序列号相同的为同一样品。		

检验项目		技术要求	样品编号	检验结果	判定
一、外观和结构	1.外观和结构	产品的外观结构应满足下列要求：结构应完整、整洁；表面涂镀层应均匀，不应起泡、龟裂、脱落和磨损；不应有明显的凹痕、破损、划痕、变形和污染等；金属零部件不	001		

检验项目		技术要求	样品编号	检验结果	判定
		应有腐蚀及其他机械损伤；设备的零部件连接应紧固无松；应有铭牌或标牌或商标。			
二、性能及功能检查	1.分辨率	产品可正确识别分辨率可分为2个等级，见下表。其中最低分辨率为15mil。 ——2级为推荐选用； ——1级为优先选用。 手持式条码扫描设备 1级: 10mil 2级: 15mil； 固定式条码扫描设备 1级: 10mil 2级: 15mil； 自助终端条码扫描设备 1级: 10mil 2级: 15mil。	001		
	2.解码能力	产品解码能力分为2个等级。见下表。 ——2级为推荐选用； ——1级为优先选用。 手持式条码扫描设备 1级: QR和PDF417 2级: QR； 固定式条码扫描设备 1级: QR和PDF417 2级: QR； 自助终端条码扫描设备 1级: QR和PDF417 2级: QR。	001		
	3.景深	产品景深分为2个等级，见下表。 ——2级为推荐选用； ——1级为优先选用。 手持式条码扫描设备 1级: 60mm～160mm 2级: 80mm～140mm； 固定式条码扫描设备 1级: 20mm～200mm 2级: 30mm～90mm； 自助终端条码扫描设备 1级: 20mm～160mm 2级: 40mm～120mm。	001		
	4.识读角度	产品（含手持式条码扫描设备、固定式条码扫描设备、自助终端条码扫描设备）识读标准测试版条码图的角度应满足下表要求： 方向 角度 X轴偏转角 -40°～40° Y轴偏转角 -40°～40° Z轴偏转角 -180°～180°	001		

检验项目		技术要求	样品编号	检验结果	判定
	5.出错率	产品（含手持式条码扫描设备、固定式条码扫描设备、自助终端条码扫描设备）识读标准测试版条码图的出错率应小于或等于10-4。	001		
	6.纠错能力	产品（含手持式条码扫描设备、固定式条码扫描设备、自助终端条码扫描设备）识读低品质测试版条码图的拒读率应≤15%，同时不应误读。此处低品质类型包括：打印间断、倾斜、磨损等。	001		
	7.移动识读能力	产品（含手持式条码扫描设备、固定式条码扫描设备、自助终端条码扫描设备）分别沿X轴、Y轴方向进行移动识读，在准确识读的情况下，其移动速度可分为3个等级，用1、2、3表示级别： 1级 X轴≥20cm/s Y轴≥30cm/s； 2级 20cm/s＞X轴≥10cm/s 30cm/s＞Y轴≥15cm/s； 3级 10cm/s＞X轴≥5cm/s 15cm/s＞Y轴≥7cm/s。	001		
	8.识读速度	产品（含手持式条码扫描设备、固定式条码扫描设备、自助终端条码扫描设备）识读标准测试版条码图，识读时间可分为3个等级，用1、2、3表示级别： ——3级：平均识读时间500ms＜t≤1000ms，表示识读速度一般，根据情况选用； ——2级：平均识读时间300ms＜t≤500ms，表示识读速度较好，推荐选用； ——1级：平均识读时间t≤300ms，表示识读速度好，优先选用。	001		
检验环境					
受试样品运行状态					
备注	/				

检验项目		技术要求	样品编号	检验结果	判定
三、电源适应能力	1.电源适应能力	①对于交流供电的产品，按下表组合对受试样品进行试验，应能正常工作。 ②对直流供电的产品，在额定电压和额定电压偏差±5%的三个条件下，对受试样品进行试验，应能正常工作。	001		
四、安全性要求	1.接地导体及其连接的电阻	产品接地导体及其连接不应有过大的电阻。 保护连接导体的电阻不得超过0.1Ω,试验后，保护连接导体不得被损坏。 试验电流：32A 试验时间：2min	001		
	2.接触电流和保护导体电流	①设备的设计和结构应当保证接触电流或保护导体电流均不可能产生电击危险。 测试点：地（中线）—电源保护接地端子 最大接触电流：≤3.5 mA 试验电压：AC / V ②测试点：地（中线）—未连接到保护接地的可触及的零部件和电路 最大接触电流：≤0.25mA 试验电压：AC /V	001		
	3.抗电强度	设备中使用的固体绝缘应当具有足够的抗电强度。 ①试验电压施加点：电源初级—地 试验电压：AC1500V 试验时间：1min ②试验电压施加点：电源初级—次级 试验电压：AC3000V 试验时间：1min	001		
检验环境					
受试样品运行状态					
备注	/				

检验项目		技术要求	样品编号	检验结果	判定
五、环境适应性试验	1.工作温度下限试验	样品在温度为-20℃±2℃的情况下达到稳定后加电工作2h，期间扫码应正常。	002		
	2.工作温度上限试验	样品在温度为45℃±2℃的情况下达到稳定后加电工作2h，期间扫码应正常。	002		
	3.贮存温度下限试验	样品在温度为-40℃±2℃的情况下存放16h后，恢复至正常大气条件2h后进行外观和结构检查，加电工作扫码应正常。	002		
	4.贮存温度上限试验	样品在温度为60℃±2℃的情况下存放16h后，恢复至正常大气条件2h后进行外观和结构检查，加电工作扫码应正常。	002		
	5.工作条件下恒定湿热试验	样品在温度为40℃±2℃,相对湿度为90%±3%的情况下达到稳定后加电工作2h，期间扫码应正常。	002		
	6.贮存条件下恒定湿热试验	样品在温度为40℃±2℃,相对湿度为93%±3%的情况下存放48h后，恢复至正常大气条件2h后进行外观和结构检查，加电工作扫码应正常。	002		
	7.振动试验	在三个互相垂直的轴线方向进行 a.初始频率响应检查 频率范围：10Hz～55Hz 扫频速率：≤1oct/min 位移幅值：0.15mm b.定频耐久试验 频率范围：10Hz～55Hz 位移幅值：0.75mm（10Hz～25Hz） 0.15mm（25Hz～55Hz） 试验时间：(30±1)min c.扫频耐久试验 频率范围：10Hz～55Hz～10Hz 扫频速率：≤1oct/min 位移幅值：0.15mm 循环次数：5次	002		

检验项目		技术要求	样品编号	检验结果	判定
		结束后进行外观和结构检查,加电工作扫码应正常。			
	8.冲击试验	在三个互相垂直的轴线方向进行 加速度：300m/s² 脉冲宽度：11ms 次数：3次/方向　波形：半正弦波 结束后进行外观和结构检查, 加电工作扫码应正常。	002		
	9.碰撞试验	在三个互相垂直的轴线方向进行 加速度：100m/s²　脉冲宽度：16ms 次数：1000次/方向　波形：半正弦波 结束后进行外观和结构检查, 加电工作扫码应正常。	002		
	10.运输包装跌落试验	运输包装件处于准备运输状态，按GB/T 4857.2的规定进行预处理4h 包装件质量　　跌落高度 m≤<15kg　　1000mm 15 kg＜m≤30 kg　　800mm 30 kg＜m≤40 kg　　600mm m＞40 kg　　450mm 任选四面跌落,　　每面跌落一次, 结束后检查包装件损坏情况，并对样品进行外观和结构检查, 样品加电工作扫码正常。	002		
检验环境					
受试样品运行状态					
备注	/				

检验项目		技术要求	样品编号	检验结果	判定	测量不确定度（dB）
六、电磁兼容性检验	1.1GHz以下辐射骚扰	应符合GB/T 9254-2008中1GHz以下辐射骚扰限值要求。	003			
	2.静电放电抗扰度	应符合GB/T 17618-2015第10条表1的规定（接触放电2kV、4kV，空气放电2kV、4kV、8kV），达到性能判据B的要求。	003			
	3.连续波辐射骚扰抗扰度	应符合GB/T 17618-2015第10条表1的规定（试验电压3V/m），达到性能判据A的要求。	003			
	4.工频磁场抗扰度	应符合GB/T 17618-2015第10条表1的规定（磁场强度1A/m），达到性能判据A的要求。	003			
检验环境						
受试样品运行状态						
备注	/					

样品照片

图1 铭牌

图2 样品外观

图3 接口

【====报告内容结束====】

附录F　密码模块自评估报告模板

密码模块检测
现场自评估报告

自评估单位信息	
自评估单位名称 （单位盖章）	
联　系　人	
联 系 电 话	
电 子 邮 件	

自 评 报 告

产品名称		规格型号	
生产单位		样品数量	3 台
生产单位 地 址		测试地点	
生产日期		抽样数量	/
检验日期		抽样基数	/
检验依据	GB4943.1-2011 《信息技术设备 安全 第 1 部分：通用要求》 GB/T 2423.1-2008 《电工电子产品环境试验 第 2 部分：试验方法 试验 A：低温》 GB/T 2423.2-2008 《电工电子产品环境试验 第 2 部分：试验方法 试验 B：高温》 GB/T 2423.3-2016 《环境试验 第 2 部分：试验方法 试验 Cab：恒定湿热试验》 《电子健康卡技术规范 第 3 部分：密码模块》		
检验项目	外观和结构、功能、性能、通讯方式、高级应用编程接口、电源适应性、安全性要求、气候环境试验		
检验结论	根据检验依据和判定（参考）依据栏中所列标准及要求，对送检样品进行了外观和结构、功能、性能、通讯方式、高级应用编程接口、电源适应性、安全性要求、气候环境试验项目检验（试验），检验项目结果详见后。		
备注	/		

批准： 审核： 主检：

本次检验用主要仪器设备			
序号	**仪器设备名称**	**仪器编号**	**计量有效期**
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
此处空白			

样品分配情况		
样品编号	**样品出厂编号**	**检验项目**
001	/	外观和结构、功能、性能、通讯方式、高级应用编程接口、电源适应性、安全性要求、气候环境试验
注：下文中“样品编号”仅保留后三位序列号，与此处后三位序列号相同的为同一样品。		

检验项目		技术要求	样品编号	检验结果	判定
一、外观和结构	1.外观和结构	结构应完整、整洁；表面涂镀层应均匀，不应起泡、龟裂、脱落和磨损；不应有明显的凹痕、破损、划痕、变形和污染等；金属零部件不应有锈蚀及其他机械损伤。	001		
		终端的零部件连接应紧固无松动。			
		指示灯应有明显标识。			
		终端应有铭牌、标牌。			
二、功能		支持居民健康卡密钥管理系统通过密码机提供的灌装接口实现电子健康卡应用密钥的灌装。	001		
		支持电子健康卡管理信息系统通过密码机提供的高级应用编程接口实现居民健康卡跨域主索引 ID、电子健康卡 ID、有效性信息等的生成、验证和加解密功能。	001		
三、性能		密码模块高级应用编程接口应支持 1000 并发调用并且在 1 秒钟内提供响应结果给电子健康卡管理信息系统。			
		测试密码卡的基础应用编程接口，调用对称算法、非对称算法等相关接口 100 万次、调用摘要算法接口 1000 万次，计算各算法的运算速度。			
四、高级应用编程接口		应符合《电子健康卡技术规范 第 3 部分：密码模块》条款 5.4 或 5.5 的要求。	001		
五、密码卡基础应用编程接口		应符合《电子健康卡技术规范 第 3 部分：密码模块》条款 5.6 的要求。	001		
六、通讯方式		密码机应具有 RJ45 以太网口，可采用 TCP/IP 协议进行数据通讯。密码卡应通过 PCI-E 或 MINI PCI-E 物理接口与主机进行数据通信。	001		
检验环境					
受试样品运行状态					
备注		/			

检验项目		技术要求	样品编号	检验结果	判定
一、外观和结构	1.外观和结构	结构应完整、整洁；表面涂镀层应均匀，不应起泡、龟裂、脱落和磨损；不应有明显的凹痕、破损、划痕、变形和污染等；金属零部件不应有锈蚀及其他机械损伤。	001		
		终端的零部件连接应紧固无松动。			
		指示灯应有明显标识。			
		终端应有铭牌、标牌。			
二、功能		支持居民健康卡密钥管理系统通过密码机提供的灌装接口实现电子健康卡应用密钥的灌装。	001		
		支持电子健康卡管理信息系统通过密码机提供的高级应用编程接口实现居民健康卡跨域主索引 ID、电子健康卡 ID、有效性信息等的生成、验证和加解密功能。	001		
三、性能		密码模块高级应用编程接口应支持 1000 并发调用并且在 1 秒钟内提供响应结果给电子健康卡管理信息系统。			
		测试密码卡的基础应用编程接口，调用对称算法、非对称算法等相关接口 100 万次、调用摘要算法接口 1000 万次，计算各算法的运算速度。			
四、高级应用编程接口		应符合《电子健康卡技术规范 第 3 部分：密码模块》的要求。	001		
五、基础应用编程接口		应符合《电子健康卡技术规范 第 3 部分：密码模块》的要求。	001		
六、通讯方式		密码机应具有 RJ45 以太网口，可采用 TCP/IP 协议进行数据通讯。密码卡应通过 PCI-E 或 MINI PCI-E 物理接口与主机进行数据通信。	001		
检验环境					
受试样品运行状态					
备注		/			

检验项目		技术要求	样品编号	检验结果	判定
七、电源适应能力	1.电源适应能力	密码机应能在 220V ± 22V、50Hz ±1Hz 条件下正常工作。 密码卡应能在 12V 或 3.3V 条件下正常工作。	001		
八、安全性要求	1. 接触电流和保护导体电流（接触电流）	应符合 GB 4943.1-2011 第 5.1 条款的相关要求：设备的设计和结构应当保证接触电流或保护导体电流均不可能产生电击危险。 电源保护接地端子 最大接触电流：≤3.5 mA 试验电压：AC264V	001		
	2．抗电强度	应符合 GB 4943.1-2011 第 5.2 条款的相关要求：设备中使用的固体绝缘应当具有足够的抗电强度。 试验电压施加点：电源初级—地 试验电压：AC1500V 试验时间：1min	001		
	3.接地导体及其连接的电阻（接地电阻）	应符合 GB 4943.1-2011 第 2.6.3.4 条款的相关要求：保护连接导体的电阻不得超过 0.1Ω,试验后，保护连接导体不得被损坏。 试验电流：32A 试验时间：2min	001		
检验环境					
受试样品运行状态					
备注	/				

检验项目		技术要求	样品编号	检验结果	判定
九、环境适应性试验	1.工作温度下限试验	样品在温度为 0℃±2℃的情况下达到稳定后加电 Ping 网口登录管理界面工作 2h 应正常。	002		
	2.贮存温度下限试验	样品在温度为-10℃±2℃的情况下存放 16h 后，恢复至正常大气条件 2h 后进行外观和结构检查，加电工作 Ping 网口登录管理界面应正常。	002		
	3.工作温度上限试验	样品在温度为 40℃±2℃的情况下达到稳定后加电 Ping 网口登录管理界面工作 2h 应正常。	002		
	4.贮存温度上限试验	样品在温度为 45℃±2℃的情况下存放 16h 后，恢复至正常大气条件 2h 后进行外观和结构检查，加电工作 Ping 网口登录管理界面应正常。	002		
	5.工作恒定湿热试验	样品在温度为 40℃±2℃,相对湿度为 80%±3%的情况下达到稳定后加电 Ping 网口登录管理界面工作 2h 应正常。	002		
	6.贮存恒定湿热试验	样品在温度为 45℃±2℃,相对湿度为 90%±3%的情况下存放 48h 后，恢复至正常大气条件 2h 后进行外观和结构检查，加电工作 Ping 网口登录管理界面应正常。	002		
检验环境					
受试样品运行状态					
备注	/				

检验项目		技术要求	样品编号	检验结果	判定
一、外观和结构	1.外观和结构	结构应完整、整洁；表面涂镀层应均匀，不应起泡、龟裂、脱落和磨损；不应有明显的凹痕、破损、划痕、变形和污染等；金属零部件不应有锈蚀及其他机械损伤。	001		
		终端的零部件连接应紧固无松动。			
		指示灯应有明显标识。			
		终端应有铭牌、标牌。			
二、功能		支持居民健康卡密钥管理系统通过密码机提供的灌装接口实现电子健康卡应用密钥的灌装。	001		
		支持电子健康卡管理信息系统通过密码机提供的高级应用编程接口实现居民健康卡跨域主索引 ID、电子健康卡 ID、有效性信息等的生成、验证和加解密功能。	001		
三、性能		密码模块高级应用编程接口应支持 1000 并发调用并且在 1 秒钟内提供响应结果给电子健康卡管理信息系统。			
		测试密码卡的基础应用编程接口，调用对称算法、非对称算法等相关接口 100 万次、调用摘要算法接口 1000 万次，计算各算法的运算速度。			
四、高级应用编程接口		应符合《电子健康卡技术规范 第 3 部分：密码模块》条款 5.4 或 5.5 的要求。	001		
五、密码卡基础应用编程接口		应符合《电子健康卡技术规范 第 3 部分：密码模块》条款 5.6 的要求。	001		
六、通讯方式		密码机应具有 RJ45 以太网口，可采用 TCP/IP 协议进行数据通讯。密码卡应通过 PCI-E 或 MINI PCI-E 物理接口与主机进行数据通信。	001		
检验环境					
受试样品运行状态					
备注		/			

检验项目		技术要求	样品编号	检验结果	判定
七、电源适应能力	1.电源适应能力	密码机应能在 220V ± 22V、50Hz ±1Hz 条件下正常工作。 密码卡应能在 12V 或 3.3V 条件下正常工作。	001		
八、安全性要求	1. 接触电流和保护导体电流（接触电流）	应符合 GB 4943.1-2011 第 5.1 条款的相关要求：设备的设计和结构应当保证接触电流或保护导体电流均不可能产生电击危险。 电源保护接地端子 最大接触电流：≤3.5 mA 试验电压：AC264V	001		
	2．抗电强度	应符合 GB 4943.1-2011 第 5.2 条款的相关要求：设备中使用的固体绝缘应当具有足够的抗电强度。 试验电压施加点：电源初级—地 试验电压：AC1500V 试验时间：1min	001		
	3.接地导体及其连接的电阻（接地电阻）	应符合 GB 4943.1-2011 第 2.6.3.4 条款的相关要求：保护连接导体的电阻不得超过 0.1Ω,试验后，保护连接导体不得被损坏。 试验电流：32A 试验时间：2min	001		
检验环境					
受试样品运行状态					
备注	/				

检验项目		技术要求	样品编号	检验结果	判定
九、环境适应性试验	1.工作温度下限试验	样品在温度为 0℃±2℃的情况下达到稳定后加电 Ping 网口登录管理界面工作 2h 应正常。	002		
	2.贮存温度下限试验	样品在温度为-10℃±2℃的情况下存放 16h 后，恢复至正常大气条件 2h 后进行外观和结构检查，加电工作 Ping 网口登录管理界面应正常。	002		
	3.工作温度上限试验	样品在温度为 40℃±2℃的情况下达到稳定后加电 Ping 网口登录管理界面工作 2h 应正常。	002		
	4.贮存温度上限试验	样品在温度为 45℃±2℃的情况下存放 16h 后，恢复至正常大气条件 2h 后进行外观和结构检查，加电工作 Ping 网口登录管理界面应正常。	002		
	5.工作恒定湿热试验	样品在温度为 40℃±2℃,相对湿度为 80%±3%的情况下达到稳定后加电 Ping 网口登录管理界面工作 2h 应正常。	002		
	6.贮存恒定湿热试验	样品在温度为 45℃±2℃,相对湿度为 90%±3%的情况下存放 48h 后，恢复至正常大气条件 2h 后进行外观和结构检查，加电工作 Ping 网口登录管理界面应正常。	002		
检验环境					
受试样品运行状态					
备注	/				

样品照片

图1 铭牌

图2 样品外观

图3 接口

【====报告内容结束====】

《电子健康卡建设与管理指南》材料三

电子健康卡跨域主索引及跨域认证技术要求

（2.0 版）

国家卫生健康委统计信息中心

2022 年 3 月

目录

1　电子健康卡跨域主索引服务

1.1　概述

电子健康卡跨域主索引服务是实现全国、省级或市级区域范围内居民信息统一识别的独立的索引信息体系。基于本服务可实现对不同区域、各类居民标识证卡的统一注册管理。

所辖电子健康卡管理信息系统通过电子健康卡跨域主索引服务提交注册电子健康卡的身份信息进行人员主索引注册。其他系统，如：医疗卫生机构索引（卡）应用系统、妇幼保健卡应用系统、计划免疫卡应用系统、全民健康信息平台等等可从本服务获取和应用电子健康卡跨域主索引与居民身份信息。

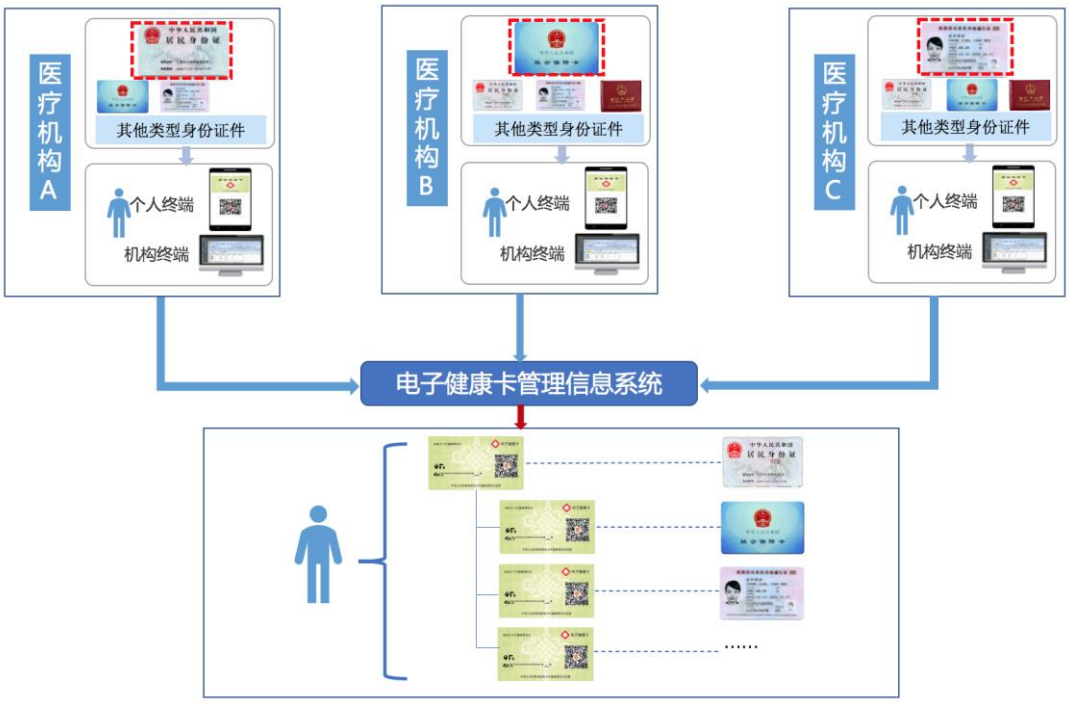


图 1.1 基于电子健康卡跨域主索引整合概念模型

本方案预期读者包括电子健康卡跨域主索引服务、电子健康卡管理信息系统；国家、省级医疗健康信息平台、电子健康卡（全民健康信息平台、区域卫生信息平台、人口健康信息平台）的管理人员、设计人员、实施人员以及注册、使用跨域主索引服务的用户团体。

1.2　需求分析

1.2.1业务需求

医疗健康信息互联互通是一项重要的民生工程，实现互联互通最核心的工作是在跨域（指不同身份标识域、跨县市区域、全省、全国，下同）范围内建立对居民个人身份的统一标识，并应用于建立跨域查询的电子健康卡ID。这项工程可以满足居民个人、医疗卫生机构以及医疗卫生管理机构的实际需求。

为建立跨域统一的电子健康卡ID，需整合不同区域的健康卡及其它标识域的个人基本信息，形成不同标识域、跨县市区域、全省乃至全国范围内唯一索引（跨域主索引或称企业级主索引(EMPI)，下称人员主索引），首先由电子健康卡管理信息系统从各医疗卫生系统采集各业务系统身份标识数据，包括用于健康服务（含就诊服务）的各类卡片、身份证、军官证、社保号、归国华侨证等身份标识卡证的标识号以及居民个人基本信息以及社会学信息。其次需要从各业务系统身份标识数据中提取关键信息，按照特定规则和策略生成电子健康卡ID，然后由电子健康卡管理信息系统使用电子健康卡ID、居民身份信息向电子健康卡跨域主索引服务注册，得到人员主索引。并由电子健康卡跨域主索引服务对人员主索引进行管理和维护。

通过电子健康卡跨域主索引服务，电子健康卡管理信息系统以及其他系统可进行跨标识域的索引、居民信息的查询和应用。

通过电子健康卡跨域主索引服务，可进一步满足整合不同标识域的多种条线业务，实现跨标识域的卫生信息互联互通；优化医疗业务流程，实现跨域诊疗，进而满足居民接受跨区域医疗健康服务的需求。

1.2.2功能需求

1.2.2.1 功能需求概述

本服务依托于电子健康卡管理信息系统可以向不同地区的医院就诊卡管系统、妇幼保健卡管系统、计划免疫卡管系统、医联卡管系统和其他卡管系统等采集个人信息，而这些信息包含了所在领域的个人标识。同时，本服务提供全国唯一的主索引信息，供国家级、省级卫生信息平台、医疗卫生机构和卫生管理机构信息系统使用，以支持不同的应用对统一个人标识及个人信息的使用需求。

同时本服务可对外部应用系统提供索引服务，满足不同业务系统之间索引互认需求。系统可提供索引监管服务功能，使用户能直观、清晰地了解到索引建设、生成、匹配情况。

电子健康卡管理信息系统可调用索引注册服务，通过已生成的电子健康卡ID注册生成电子健康卡跨域主索引服务中的人员主索引。实现居民可通过智能手机等方式进行医疗就诊、获取公共卫生服务，享受政府、社区、医疗卫生机构以及社会福利机构所提供的健康服务。电子健康卡与实体居民健康卡同样应用本服务提供的一致化的主索引服务，实现卫生健康“一卡通”。

1.2.2.2 角色分析

系统管理员：对索引进行管理。对平台进行配置、保障平台正常运行的系统管理人员；

索引服务使用者：使用系统提供的索引服务。电子健康卡管理信息系统、全民健康信息平台、医疗卫生信息系统（HIS、公共卫生信息系统等）

1.2.2.3 系统用例

平台主要用例图如下：

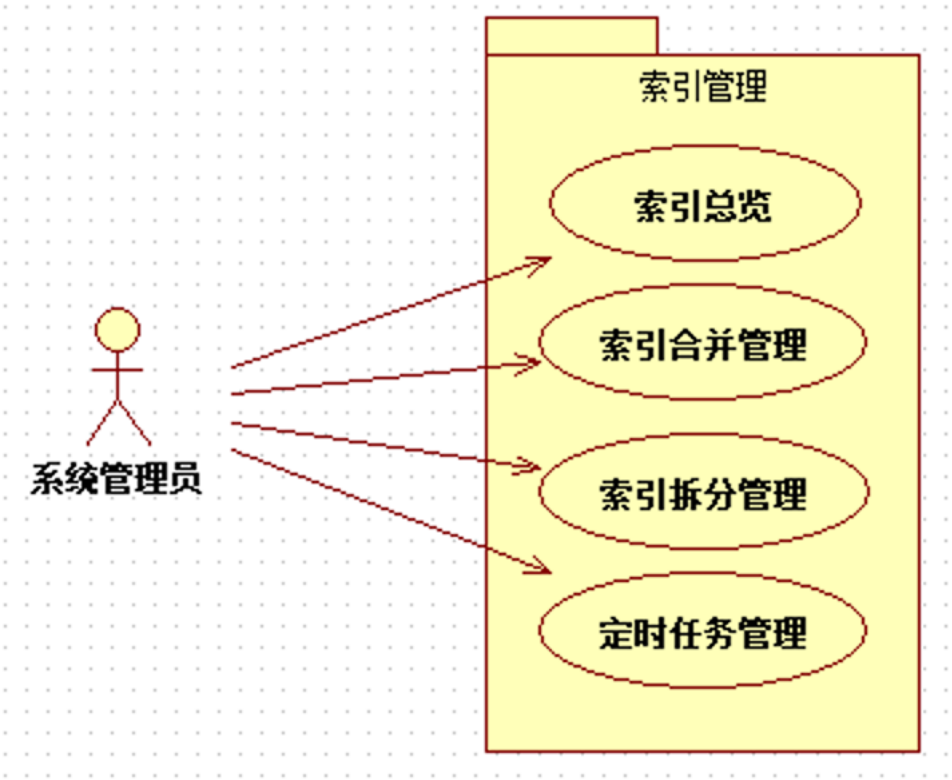


图 1.2 跨域主索引系统主要用例图

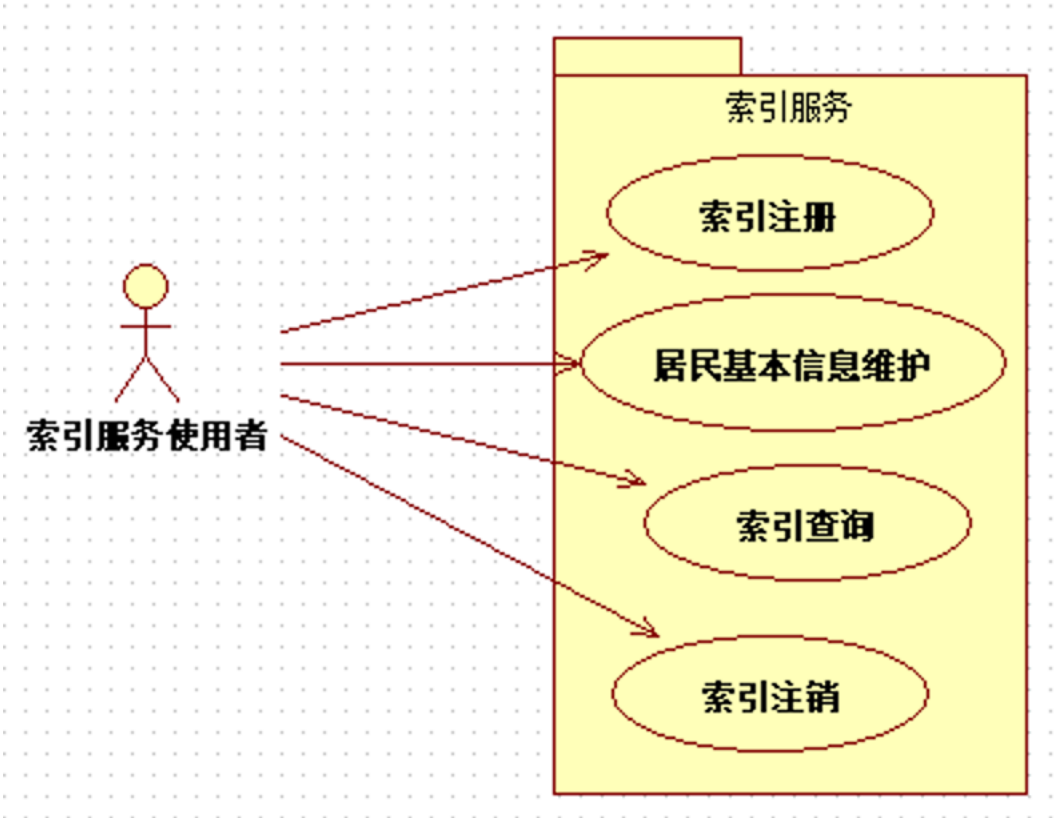


图 1.3 跨域主索引系统主要用例图

1.3 技术架构

1.3.1 总体技术架构

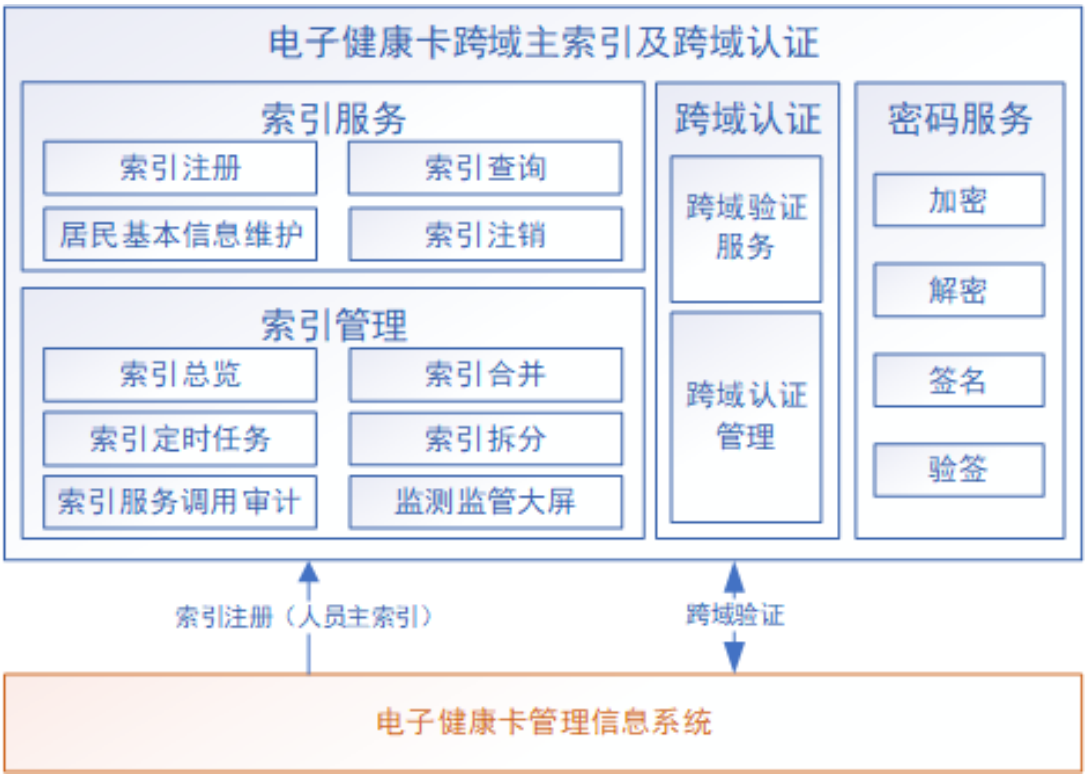


图 1.4电子健康卡跨域主索引及跨域认证技术架构图

在电子健康卡跨域主索引服务的架构中，人员主索引是信息交互的交叉点，它的存在能确保跨机构、跨部门之间及时、精准的信息调度。

1.3.2 关键技术

1) 建立电子健康卡跨域主索引服务负责索引管理，包括居民基本信息及主索引信息的注册、更新、合并、查询。
2) 将不同地点机构、不同业务条线系统、不同标识体系视为不同的标识域，实现居民在不同地点机构、不同业务条线应用产生的健康医疗事件关键信息的融合。
3) 通过建立基于规则的个人身份匹配引擎，实现对不同记录间个人身份匹配度的计算，并依据规则实现个人信息自动合并或手动拆分。
4) 整个索引体系满足分布式结构，可实现强中心化和弱中心化两种模式。

5) 所有的核心信息采用国家自有加密算法生成ID。

1.4 总体设计

1.4.1功能服务

1.4.1.1 索引管理

包括如下功能模块：索引总览、索引服务调用审计、监测监管大屏、索引合并、索引拆分、索引定时任务。

（1）索引总览：展示系统中人员主索引信息及居民基本信息概览。

（2）索引服务调用审计：展示索引服务调用日志记录。

（3）监测监管大屏：展示索引数据概览，对服务调用情况进行监控统计。

（4）索引合并：建立索引匹配规则，基于匹配规则周期性轮询索引信息，对满足规则的自动合并；支持查看合并调用记录和合并总览。

（5）索引拆分：基于规则的匹配度查询，支持个人信息的手动拆分。

（6）索引定时任务：设置索引计划任务的执行规则。

1.4.1.2 索引服务

主要提供给第三方应用系统调用。包括如下功能模块：索引注册、索引查询、索引注销。

（1）索引注册：支持单个索引和批量索引信息注册。人员主索引包括人员主索引ID、证件类型、证件号码、索引父ID、居民基本信息等。居民基本信息包括姓名、性别、身份证信息、民族、手机号码、健康档案管理地行政区域编码前六位（优先使用居民常住地，其次为户籍地）等信息。

注：健康档案管理地为必须项，后期支撑健康档案跨地域迁入（出）、调阅等场景使用。

（2）居民基本信息维护：提供居民基本信息的添加、修改服务。

（3）索引查询：提供给第三方应用系统查询索引信息，支持精准查询和模糊查询。

（4）索引注销：提供给第三方应用系统注销索引信息，支持精准注销和批量注销。

1.5 主索引设计规范

1.5.1 人员主索引 ID 生成方案

人员主索引ID即为电子健康卡管理信息系统中的电子健康卡ID。

电子健康卡ID的详细生成方案可参见“电子健康卡密码模块接口及卡管系统接入认证技术要求”。

其中：

——证件号码：居民有效身份证件号码；

——证件类型：在WS364.3-2011卫生信息数据元值域代码 第3部分:人口学及社会经济学特征4.1.1 CV02.01.101身份证件类别代码表的基础上增加08出生医学证明，证件类型代码见表1：

表 1 证件类型代码表

证件类型	值含义
01	居民身份证
02	居民户口簿
03	护照
04	军官证
05	驾驶证
06	港澳居民来往内地通行证
07	台湾居民来往内地通行证
08	出生医学证明
99	其他法定有效证件

2 电子健康卡跨域认证服务

为实现电子健康码在全国范围内一码通用、跨地域识别，电子健康卡管理信息系统需要通过电子健康卡跨域主索引及跨域认证系统中的跨域认证服务来实现区域范围内的电子健康卡跨域验证。

2.1 总体架构

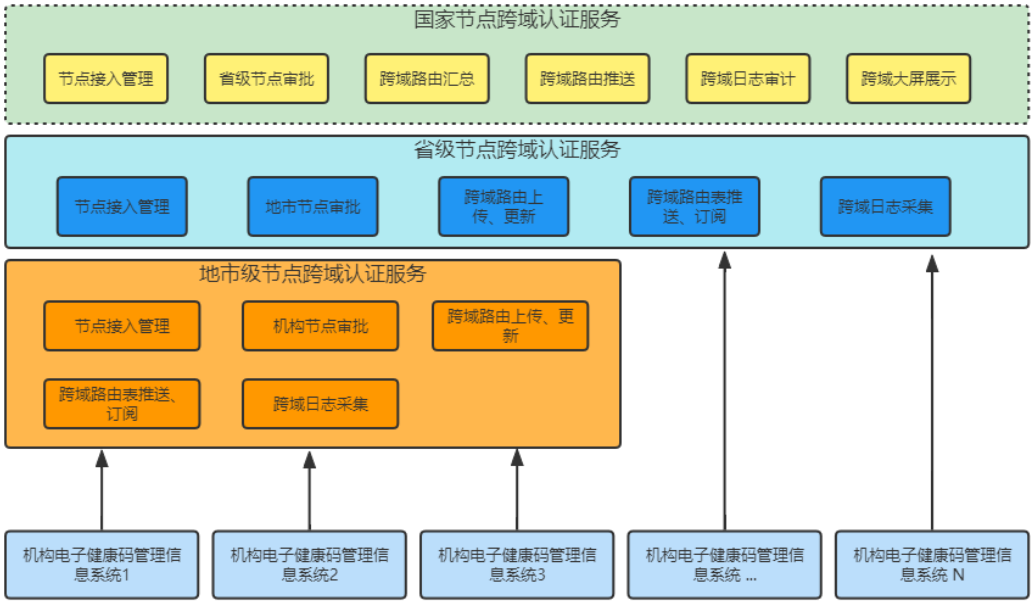


图 2.1 跨域认证服务总体架构图

国家节点跨域认证服务提供了省级卡管节点的接入管理、审批功能，全国卡管节点路由汇总、推送功能，跨域日志审计及跨域大屏展示功能。

省级、地市级节点跨域认证服务提供节点接入管理、审批功能，跨域路由上传、更新、订阅功能及跨域日志采集功能。

机构级节点提供的功能详见2.2。

在跨域认证服务架构中，各级节点应向上一级节点进行跨域认证服务注册，节点可为省级、地市级或机构节点，最终统一将各地节点路由信息汇聚到国家节点，形成一张全国整体节点路由表，再由各级节点以订阅服务的方式向上级节点获取最新路由表，通过互联网，以实现卡管与卡管间的跨域认证服务。具体跨域认证业务流程见图2.2

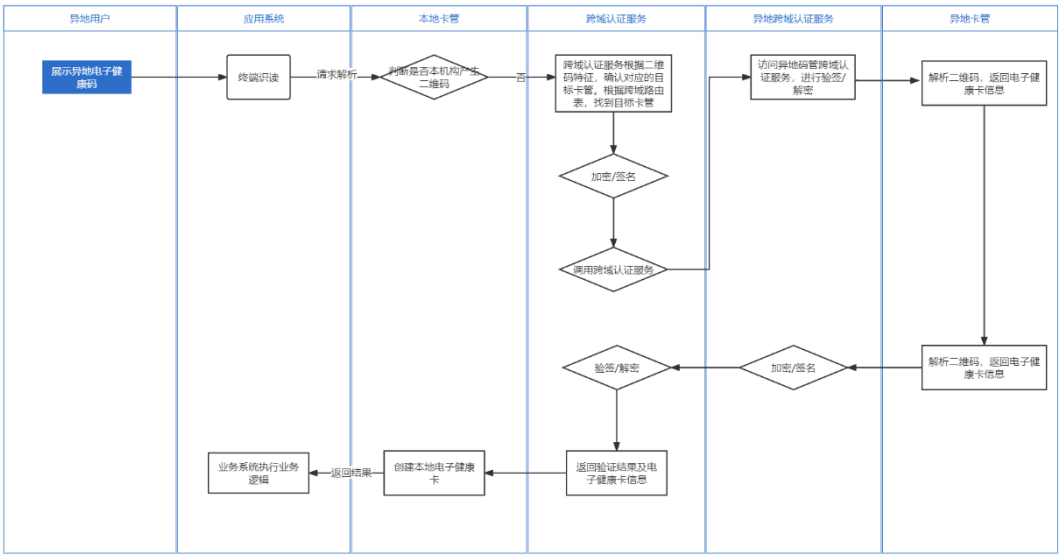


图 2.2跨域认证业务流程图

2.2 跨域认证技术要求

2.2.1 跨域节点管理

电子健康卡管理信息系统在上线启动后应当将本卡管系统信息向本级部署的电子健康卡跨域主索引及跨域认证系统注册，再通过跨域认证服务向上级节点跨域认证服务注册，使上级节点跨域认证服务能够识别到本级节点。跨域认证服务对于新节点的注册、更新，需要上送的信息包括有：卡管系统联网接入地址、联网接入应用编号、联网接入应用密钥、卡管节点入网编码。具体参数要求详见附录 A。

电子健康卡管理信息系统通过电子健康卡跨域主索引及跨域认证系统的跨域认证服务向上级节点跨域认证服务进行注册后，跨域认证服务应提供全网节点路由信息、存储和更新功能，并定期向上级节点进行路由信息订阅，同时应提供跨域认证服务节点心跳上传、跨域日志采集、跨域报表上传功能。

2.2.2 跨域验证服务

电子健康卡管理信息系统被请求识读电子健康卡二维码时，若发现非本地卡管发出的二维码，此时本地电子健康卡管理信息系统应当通过电子健康卡跨域主索引及跨域认证系统的跨域认证服务进行解析，跨域认证服务根据二维码上的卡管标识将请求路由至

对应的发卡卡管的跨域认证服务节点，在发卡卡管中进行数据验证，并且在验证成功后，将原路返回对应的电子健康卡信息，包括：发卡机构名称、发卡机构代码、证件类型、证件号、用户姓名、电子健康卡 ID 等。具体参数要求详见附录 A。

2.3 跨域认证管理

跨域认证服务（省级、地市级节点）应对下级节点的注册信息进行审批，注册信息包括：卡管联网接入地址、联网接入应用编号、联网接入应用密钥、卡管节点入网编码。在审批通过后，将其联网接入地址写入路由表中，各级节点仅负责维护本节点的路由表，再将路由表上传到上级节点。同时，应提供路由表订阅接口供下级卡管以T+0方式进行订阅。

国家节点仅承担各省级节点的注册审批，将各省上传的路由信息汇总，形成全国节点路由总表，供各省级节点订阅最新的路由表，并对跨域认证日志信息进行审计及监管。

3 密码服务

在进行跨域认证过程中，需要跨域认证服务通过对联网接入应用编号、联网接入应用密钥授权信息采用国密算法进行密码运算，在通信过程中对跨域认证请求进行加密和签名认证的方式，保证安全有效的跨域认证。

跨域认证服务的接入认证方案详见“电子健康卡密码模块接口及卡管系统接入认证技术要求 V1.0”。跨域认证相关接口的安全规范详见本材料附录A。

附录 A（规范性）电子健康卡跨域验证接口规范

1 前言

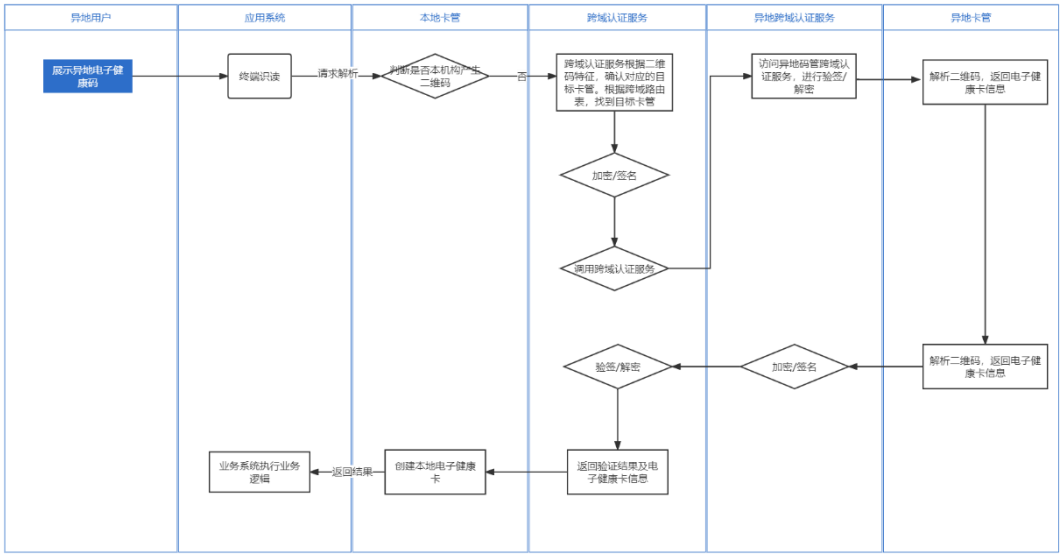
1.1 文档目的

本部分给出了跨域认证登记注册和跨域验证的实现接口。电子健康卡跨域主索引及跨域认证系统应按照此接口实现国家跨域认证平台的注册和验证，保证电子健康卡互联互通。

1.2 阅读对象

本文适用于电子健康卡开发技术人员以及对接电子健康卡技术人员阅读。

2 业务功能



跨域验证流程图请求跨域验证，参见 4.2 接口

3 接口规则

3.1 协议规则

调用方式	HTTPS
提交方式	POST
数据格式	提交和返回数据均为 JSON 格式
字符编码	统一采用 UTF-8 字符编码
判断逻辑	先判断协议字段返回，再判断业务返回，最后判断交易状态
签名算法	请求和响应均需要签名，采用 SM3 算法（或其他）
加密算法	请求和响应均需要加密，采用 SM4 算法（或其他）

3.2 参数规定

1） 日期时间格式，统一 yyyyMMddHHmmss

3.3 接口声明

接口对参数命名字母大小写敏感，要求第三方接口开发商在调用各接口时，务必按照本接口规范定义的参数名称传入，字母大小写错误将导致无法识别或数据丢失的风险。

各交易中的“返回参数”值，当交易成功时，根据返回参数结构定义的参数项返回结果；

当交易失败时，只返回公众响应参数，biz_content 中的参数均不返回。

3.4 安全规范

电子健康卡平台有提供相应的 JAVA SDK，SDK 封装与平台交互的相关逻辑，包括接口请求、报文签名、报文验签、报文加密、报文解密等，开发者只需要引入 SDK，调用相应方法，传入接口参数即可。

3.4.1 加密算法

如开发者不用 sdk，可根据 SM4 加密算法，自己加解密。以下是结合平台业务对自主加解密进行简单说明：

3.4.1.1 请求报文加密

1. 组装请求报文

根据 API 列表定义参数，整理请求报文


```
{
    "app_id": "vzusug4lhvq2enpxer",
    "biz_content":
"{\"ehealth_code\":\"C50EF5E2892CF29BDC2EFF37C4E9B36F1DA8BDC53B48F7AB5273E4D0
80CEFA08:0:7F4D9C5D163963FFF9BE8DEB29037A75::35020001001\",\"operator_id\":\"
001\",\"operator_name\":\"test\",\"out_verify_no\":\"495a8f3e994f41718b60b7f6
92fa37af\",\"out_verify_time\":\"20181227223222\",\"treatment_code\":\"010101
\"}",
    "digest_type": "SM3",
    "enc_type": "SM4",
    "method": "ehc.ehealthcode.verify",
    "term_id": "3500000104341",
    "timestamp": "1545921142502",
    "version": "1.0.0"
}
```


2. 待加密串

取出 **biz_content** 明文字段，得到待加密串明文串 jStr：

{"ehealth_code":"C50EF5E2892CF29BDC2EFF37C4E9B36F1DA8BDC53B48F7AB5273E4
D080CEFA08:0:7F4D9C5D163963FFF9BE8DEB29037A75::35020001001","operator_id":"
001","operator_name":"test","out_verify_no":"495a8f3e994f41718b60b7f692fa37
af","out_verify_time":"20181227223222","treatment_code":"010101"}

3. **报文加密密钥**

根据 **enc_type** 声明加密算法 SM4，使用 app_secret 转 16 进制，截取前面 32 位作为报文加密密钥；

42454539373543433731453231463346453837444539463731323144453331463039423933443141433830344136304242463837374332343045424230464336

4. **获取密文**

将 jStr 转为十六进制字符串（UTF-8），如下：

7B226568656616C74685F636F6465223A22433530454635453238393234632394244433245464633374334453942333646314441384244433533423438463741423532373345344430383043454641303833A303A37463444394335443136333936334646463942453844454232393033374137353A3A333530323030303130303122C226F70657261746F725F6964223A22303031222C226F70657261746F725F6E616D65223A2274657374222C226F75745F7665726966795F6E6F223A22343935613866336539393466343137313862363062376636393266613337616622C226F75745F7665726966795F74696D65223A22323031383132323732323332323222C2274726561746D656E745F636F6465223A223031303130313031227D

使用 3 获得的报文加密密钥，根据 **enc_type** 声明加密算法 SM4 加密，**将加密结果转 16 进制，再将 16 进制串转换为大写**，获得加密密文 enc_data:

E1A78A21826D512E685B599A960D7E417493315542ABB76EF85A73EF2351AEF120528E31E8EE4344FE644FD30349271F32CC6926188815B37177527C0F78722DCC85CAD4D959176E6A315173DBB9072FC0AB9359485AA6F2F905ACBD3BAD93300A43B5E9F39C3C0025B91F7CBAC3F80C49B5E2DE39BF43654C67FBF0B2094EE6A423CFF2F6630A2646AE45054EE34E87C7CD49A3162B40A0F7C5FD577D60C78135BCA117F4522001F1A49748DA2E335F02EE12011ED86C64297E59D1AA866EF9A66CE994299C0C48C83F25A086D767DCAB5A817B9F2C4AB5EAFE0A523F1CBAD1BD5C4C95F26C0219974A7BB8E122DEBC8BA6AB8DC0A386A40A4CCEF82EF5E94C71ECCEBF31974CCE1F9B8A4D2E95FA33079E4E31DAD42751AB53152AE6CCBD25BE2F481C4EAC3C89B7AF

80D6A5EBC42CB1CEC1F9C88F1173FA952CBFC80017374C77EAFD1332185D75C9D7DC95595F9
5B4499D0E9DF320C4DE97CF2469CCB9FE29F5D5DC44608E3F9B092F5E41E4AB465E1AC74FE4
DD98906A6635BF7EB291D33D0F8ADAF60A11FE6808A0F83ED143C0E574D3D8AB40B049B729C
5C464E453687F0FDA03E3CB64D13F724520B9743C7EB63489E3A7A8CDA1A88E9FAB598DBB3E
E335824252E10FC17CCAD1716555580595AE6DB41FD1259CE200849786E166970B6A0CBDA20
7FFB43E38FB82777DB1346BFDFECDE8D92A5484DF84F2B143F553E39CF649EC6E0F4ADA47EC
4C5B7826051CC211F71C8396C18C2C565EEAB4B2F7B589004F0A3DE76AEC82DE011FB1EF66E
FD762DF3BD4F8FAFA7059E2E9E9DCE6

5. **设置密文**

将加密结果 enc_data，赋值替换 **biz_content** 明文成密文


```
{
    "app_id": "vzusug4lhvq2enpxer",
    "biz_content":
"E1A78A21826D512E685B599A960D7E417493315542ABB76EF85A73EF2351AEF120528E31E
8EE4344FE644FD30349271F32CC6926188815B37177527C0F78722DCC85CAD4D959176E6A3
15173DBB9072FC0AB9359485AA6F2F905ACBD3BAD93300A43B5E9F39C3C0025B91F7CBAC3F
80C49B5E2DE39BF43654C67FBF0B2094EE6A423CFF2F6630A2646AE45054EE34E87C7CD49A
3162B40A0F7C5FD577D60C78135BCA117F4522001F1A49748DA2E335F02EE12011ED86C642
97E59D1AA866EF9A66CE994299C0C48C83F25A086D767DCAB5A817B9F2C4AB5EAFE0A523F1
CBAD1BD5C4C95F26C0219974A7BB8E122DEBC8BA6AB8DC0A386A40A4CCEF82EF5E94C71ECC
EBF31974CCE1F9B8A4D2E95FA33079E4E31DAD42751AB53152AE6CCBD25BE2F481C4EAC3C8
9B7AF80D6A5EBC42CB1CEC1F9C88F1173FA952CBFC80017374C77EAFD1332185D75C9D7DC9
5595F95B4499D0E9DF320C4DE97CF2469CCB9FE29F5D5DC44608E3F9B092F5E41E4AB465E1
AC74FE4DD98906A6635BF7EB291D33D0F8ADAF60A11FE6808A0F83ED143C0E574D3D8AB40B
049B729C5C464E453687F0FDA03E3CB64D13F724520B9743C7EB63489E3A7A8CDA1A88E9FA
B598DBB3EE335824252E10FC17CCAD1716555580595AE6DB41FD1259CE200849786E166970
B6A0CBDA207FFB43E38FB82777DB1346BFDFECDE8D92A5484DF84F2B143F553E39CF649EC6
```

```
E0F4ADA47EC4C5B7826051CC211F71C8396C18C2C565EEAB4B2F7B589004F0A3DE76AEC82D
E011FB1EF66EFD762DF3BD4F8FAFA7059E2E9E9DCE6",
        "digest_type": "SM3",
        "enc_type": "SM4",
        "method": "ehc.ehealthcode.verify",
        "term_id": "3500000104341",
        "timestamp": "1545921142502",
        "version": "1.0.0"
    }
```


3.4.1.2 返回报文解密

1. 获取响应报文


```
{
    "app_id": "vzusug4lhvq2enpxer",
    "biz_content":
"1F61C3BC533DCD0E174EBC7A6D18A18BF6F21C29476DF75976D72068D3B720903FE5FEE28471811A42D593
47761868C14E93E9FAED5FB54434CB2C47163E01B5981CA465A4E1D9C3BE1861DBA53F02A34E08204333866
CD772510BBF1BC0DFDCF4376C1278C00C004EE8266650DDB82D59AAA416F4FF71B8A0A7C52E1469341F4677
B0079C1ABB0DCE49B6C61AC4D25505B10EE25B9D6AF94E69E14938DABE2D408949F60535D805758A21D77AA
6FA5420596C0091650F3D16AEAF2B416DD5E1CB541DFD0A30451751D965CCC34007BF82A320C840A8EAB67E
42E62B912812A703CFFD76888A933B669B8B55FC9F00E0AD0E1499AC29BD506C05ED24A4BF3DBA73470E0AB
125B6368373B07CF1C24B3AFDF55C0C274D437795BA74D351382E535869844FCDE9A44A738F40C4FBB9B91B
AF8168FAE61478BAD53BF1FE1CE03B3E0CAFA52147F51EE8EA9A465AB005A6A33C98E693CB4312416107392
```

70BC58186FCAC6AEC6FD14BA8D0339255747CA18599420532A34D3D1E6C8C36D79EC3BC6675056A3D32F300B6B3735F2C1614543B7CB1CD2454D28EE53891546DF3B5EDFBFDC1DB9D2F9E4CB19A403E1F71B72D410EB0D84390C73BAC35B51BE2C74F79565169BD8F3D911DC81CDD12EA81DD30A6775C838036059060ACCAF35F7A8125E0853DC13DCA82ACFC09507A50A1D3955B21FE03A687CF07B3F9512A21DE597354E564B2619982E2A335D804A02CABBE3821FE03A687CF07B3F9512A21DE59735405CAFD378552C9F5133866260989C7708A4C347E99FB218A5E0A0040492094A03560C560AB6033FAFCFFD3BA048FB745B40C252870E9043742D3B33F8FF3C70AA9A8772CE50131D777BF300D02BC20E189883F46A308B7E08FD5C150CA094486FEDE6DC064AC9D5D92B65BA34786D0FECC4C6F75985618C6D792ABD53CF54F2E80DF8C1C5B6EEFF975D5FFF04E5CB831213A60ECBEDD7A2BEF26C491CA6C7E436C71C24AFA20D6F31A9E4AD2337E2A39B16B50EC54343A6F18261DC06B8C088F94EC15F25308AFE5686FDDE33E51F6268666E7134F896EB5CCC4A60D77789FAA819E6CA2FA063E099B1FE0EF32E369A1D2C59F2FD7EA1262DFF01D532C68971B94EC15F25308AFE5686FDDE33E51F6268666E7134F896EB5CCC4A60D77789FAAFB85DD60057073B927DBE2BACE6B0B6EB5FF5E3D517A24D35938EADD36E6BC5EAE5B325A1C968335AC1C68CAC477B9688B9AE08CE4604C082111B2E5B380E4B6208D1B304BA36D992A333F8D3D78FB0D0FF831C4CE3502372CFE5DD975879AFAF986875DC698BE17B11A09E9C938D1008D88F00F0E5E652870CC432F6AD23234EE11BD71653AAD237AC7521D59D94E68FD3742537BB24866031CE7A62E4AD327BE171E91185A868AF3D5F443FEB5E346EE6482FFC85A60B16F7FEB0C9D69FA29E47EF474157BC6FC51C17E77DF17B06C2FD5BA71C54A52E1C8BB9DF3353291C00224A38DE871C028AD0689C6BF34E2B29D526504C89C0F9E47E81F818B44A765D9EA44AA0FB5FDD6B115C80EEDF4EB5D5EE4BE22176E00A70531075E11B083D90053BF0B35B10845E99CACB9EBD390F9694CC8DD37F7FBFB82048DF3AB97B306873B7C89045F88D5219BB008FC7B766DB4FB91CBD2AA07CD63EFF61AF3602F83BF6D5E56A3F91ACC574CD80ADE0C847801B561179DB87BB024494E7A747C1E69AB01CC52ED382BBCA39D0A5894D978A8BE06863AA322855247E136C6BDD8DD3549DAA0DC4256449A5C13887241386EAC94CE8F0DAA7AE5D5777BF41BFBB74AD7",
        "digest": "45D8681184A414B406D52C4E45B38BA5D44ED2F072F85D4F3EDA8C92028E480B",
        "digest_type": "SM3",
        "enc_type": "SM4",
        "method": "ehc.ehealthcode.verify",
        "ret_code": "0000",
        "ret_msg": "交易成功",

```
    "sign": "",
    "sign_type": "",
    "timestamp": "20181227223223",
    "version": "1.0.0"
}
```

2. 获取加密密文数据 enc_data

1F61C3BC533DCD0E174EBC7A6D18A18BF6F21C29476DF75976D72068D3B720
903FE5FEE28471811A42D59347761868C14E93E9FAED5FB54434CB2C47163E01B5
981CA465A4E1D9C3BE1861DBA53F02A34E08204333866CD772510BBF1BC0DFDCF4
376C1278C00C004EE8266650DDB82D59AAA416F4FF71B8A0A7C52E1469341F4677
B0079C1ABB0DCE49B6C61AC4D25505B10EE25B9D6AF94E69E14938DABE2D408949
F60535D805758A21D77AA6FA5420596C0091650F3D16AEAF2B416DD5E1CB541DFD
0A30451751D965CCC34007BF82A320C840A8EAB67E42E62B912812A703CFFD7688
8A933B669B8B55FC9F00E0AD0E1499AC29BD506C05ED24A4BF3DBA73470E0AB125
B6368373B07CF1C24B3AFDF55C0C274D437795BA74D351382E535869844FCDE9A4
4A738F40C4FBB9B91BAF8168FAE61478BAD53BF1FE1CE03B3E0CAFA52147F51EE8
EA9A465AB005A6A33C98E693CB431241610739270BC58186FCAC6AEC6FD14BA8D0
339255747CA18599420532A34D3D1E6C8C36D79EC3BC6675056A3D32F300B6B373
5F2C1614543B7CB1CD2454D28EE53891546DF3B5EDFBFDC1DB9D2F9E4CB19A403E
1F71B72D410EB0D84390C73BAC35B51BE2C74F79565169BD8F3D911DC81CDD12EA
81DD30A6775C838036059060ACCAF35F7A8125E0853DC13DCA82ACFC09507A50A1
D3955B21FE03A687CF07B3F9512A21DE597354E564B2619982E2A335D804A02CAB
BE3821FE03A687CF07B3F9512A21DE59735405CAFD378552C9F5133866260989C7
708A4C347E99FB218A5E0A0040492094A03560C560AB6033FAFCFFD3BA048FB745
B40C252870E9043742D3B33F8FF3C70AA9A8772CE50131D777BF300D02BC20E189
883F46A308B7E08FD5C150CA094486FEDE6DC064AC9D5D92B65BA34786D0FECC4C
6F75985618C6D792ABD53CF54F2E80DF8C1C5B6EEFF975D5FFF04E5CB831213A60

ECBEDD7A2BEF26C491CA6C7E436C71C24AFA20D6F31A9E4AD2337E2A39B16B50EC
54343A6F18261DC06B8C088F94EC15F25308AFE5686FDDE33E51F6268666E7134F
896EB5CCC4A60D77789FAA819E6CA2FA063E099B1FE0EF32E369A1D2C59F2FD7EA
1262DFF01D532C68971B94EC15F25308AFE5686FDDE33E51F6268666E7134F896E
B5CCC4A60D77789FAAFB85DD60057073B927DBE2BACE6B0B6EB5FF5E3D517A24D3
5938EADD36E6BC5EAE5B325A1C968335AC1C68CAC477B9688B9AE08CE4604C0821
11B2E5B380E4B6208D1B304BA36D992A333F8D3D78FB0D0FF831C4CE3502372CFE
5DD975879AFAF986875DC698BE17B11A09E9C938D1008D88F00F0E5E652870CC43
2F6AD23234EE11BD71653AAD237AC7521D59D94E68FD3742537BB24866031CE7A6
2E4AD327BE171E91185A868AF3D5F443FEB5E346EE6482FFC85A60B16F7FEB0C9D
69FA29E47EF474157BC6FC51C17E77DF17B06C2FD5BA71C54A52E1C8BB9DF33532
91C00224A38DE871C028AD0689C6BF34E2B29D526504C89C0F9E47E81F818B44A7
65D9EA44AA0FB5FDD6B115C80EEDF4EB5D5EE4BE22176E00A70531075E11B083D9
0053BF0B35B10845E99CACB9EBD390F9694CC8DD37F7FBFB82048DF3AB97B30687
3B7C89045F88D5219BB008FC7B766DB4FB91CBD2AA07CD63EFF61AF3602F83BF6D
5E56A3F91ACC574CD80ADE0C847801B561179DB87BB024494E7A747C1E69AB01CC
52ED382BBCA39D0A5894D978A8BE06863AA322855247E136C6BDD8DD3549DAA0DC
4256449A5C13887241386EAC94CE8F0DAA7AE5D5777BF41BFBB74AD7

3. **报文解密密钥**

根据 **enc_type** 声明加密算法 SM4，使用 app_secret 转 16 进制，截取前面 32 位作为报文加密密钥；

42454539373543433731453231463346453837444539463731323144453331463039423
93344314143383034413630424246383737433234304542423046433 6

4. **获取明文**

根据 enc_type 声明加密算法，使用 3.获取的报文解密密钥，解密 enc_data 获取 JSON 字符串明文十六进制串

7B2262697274685F706C616365223A22222C22626972746864617922 3A22313939303038323022C22636172645F6E6F223A224B3532343537333135 222C22636172645F74797065223A223031222C22656865616C74685F636172 645F6964223A22433530454635453238393243463239424443324546463337 43344539423336463144413842444335334234384637414235323733453444 303830434546413038222C226578747261223A227B5C22626A6A6269655C22 3A5C225C222C5C22667A786268305C223A5C2230315C222C5C22667A786D63 305C223A5C22E79C81E58CBBE4BF9DE4B8ADE5BF835C222C5C226772736665 6E5C223A5C225C222C5C22677273666D635C223A5C225C222C5C22677A7A74 30305C223A5C2230315C222C5C22677A7A746D635C223A5C22E59CA8E8818C E4BABAE591985C222C5C2269637A7462685C223A5C22325C222C5C2269637A 746D635C223A5C22E69C89E695885C222C5C226964303030305C223A5C2233 353033323231393930303832303731355C227D222C2269645F6E6F223A22 333530333232313939303038323037373135222C2269645F74797065223A22 3031222C226D696E6465785F6964223A22363341413934333842344346363 1334434304436363138383337304232374233423134314146413642393233 38423244344245363831444135363044324533312222C226D6F62696C655F7068 6F6E65223A22313336343630333230363522 2C22757365725F6E616D65223A 22E99988E4BF8AE6B5B7222C22757365725F736578223A2231222C22786D61 6E5F6964223A22306561353230393 32D303636622D343939362D393265372D 363632633135326430333034227D

将十六进制转明文

{"birth_place":"","birthday":"19900820","card_no":"K52457315","card_typ e":"01","ehealth_card_id":"C50EF5E2892CF29BDC2EFF37C4E9B36F1DA8BDC53B48F7AB 5273E4D080CEFA08","extra":"{\"bjjbie\":\"\",\"fzxbh0\":\"01\",\"fzxmc0\":\" 省医保中心\",\"grsfen\":\"\",\"grsfmc\":\"\",\"gzzt00\":\"01\",\"gzztmc\":\ "在职人员\",\"icztbh\":\"2\",\"icztmc\":\"有效\",\"id0000\":\"3503221990082

07715\"}","id_no":"350322199008207715","id_type":"01","mindex_id":"63AA9438B4CF613D40D66188370B27B3B141AFA6B9238B2D4BE681DA560D2E31","mobile_phone":"13646032065","user_name":"陈俊海","user_sex":"1","xman_id":"0ea52093-066b-4996-92e7-662c152d0304"}

5. 设置明文

将 jStr 转换为 JSON 赋值 param，获取解密后返回报文


```
{
    "app_id": "vzusug4lhvq2enpxer",
    "biz_content":
"{\"birth_place\":\"\",\"birthday\":\"19900820\",\"card_no\":\"K52457315\",\"card_type\":\"01\",\"ehealth_card_id\":\"C50EF5E2892CF29BDC2EFF37C4E9B36F1DA8BDC53B48F7AB5273E4D080CEFA08\",\"extra\":\"{\\\"bjjbie\\\":\\\"\\\",\\\"fzxbh0\\\":\\\"01\\\",\\\"fzxmc0\\\":\\\"省医保中心\\\",\\\"grsfen\\\":\\\"\\\",\\\"grsfmc\\\":\\\"\\\",\\\"gzzt00\\\":\\\"01\\\",\\\"gzztmc\\\":\\\"在职人员\\\",\\\"icztbh\\\":\\\"2\\\",\\\"icztmc\\\":\\\"有效\\\",\\\"id0000\\\":\\\"350322199008207715\\\"}\",\"id_no\":\"350322199008207715\",\"id_type\":\"01\",\"mindex_id\":\"63AA9438B4CF613D40D66188370B27B3B141AFA6B9238B2D4BE681DA560D2E31\",\"mobile_phone\":\"13646032065\",\"user_name\":\"陈俊海\",\"user_sex\":\"1\",\"xman_id\":\"0ea52093-066b-4996-92e7-662c152d0304\"}",
    "digest": "45D8681184A414B406D52C4E45B38BA5D44ED2F072F85D4F3EDA8C92028E480B",
    "digest_type": "SM3",
    "enc_type": "SM4",
    "method": "ehc.ehealthcode.verify",
    "ret_code": "0000",
    "ret_msg": "交易成功",
    "sign": "",
    "timestamp": "20181227223223",
```

```
    "version": "1.0.0"
}
```

备注：

SM4 加密参数;

加密算法 SM4/ECB;

填充 16 位补位填充。

3.4.2 摘要算法

如开发者不用 SDK，可根据规则自己拼写摘要方法。以下是结合平台业务对自主摘要进行简单说明：

3.4.2.1 请求报文-摘要值生成流程

1. 筛选

获取所有请求参数，不包括字节类型参数，如文件、字节流，剔除 digest 字段。

(app_id、biz_content、digest_type、enc_type、method、term_id、timestamp、version)

2. 排序

将筛选的参数按照第一个字符的键值 ASCII 码递增排序（字母升序排序），如果遇到相同字符则按照第二个字符的键值 ASCII 码递增排序，以此类推。

3. 拼接

将排序后的参数与其对应值，组合成“参数=参数值”的格式，并且把这些参数用&字符连接起来，最后拼接上应用密钥 app_secret，格式如下

“…参数=参数值&app_secret=你的密钥”

此时生成的字符串为待签名字符串，对待签名字符串 SM3 运算，即是摘要（digest）的值。

注意：“DIGEST”参数不参与签名

例如下面的请求示例，参数值都是示例，开发者参考格式即可：


```
{
    "app_id": "vzusug4lhvq2enpxer",
    "biz_content": "E1A78A21826D512E685B599A960D7E417493315542ABB76E
F85A73EF2351AEF120528E31E8EE4344FE644FD30349271F32CC6926188815B3717752
7C0F78722DCC85CAD4D959176E6A315173DBB9072FC0AB9359485AA6F2F905ACBD3BAD
93300A43B5E9F39C3C0025B91F7CBAC3F80C49B5E2DE39BF43654C67FBF0B2094EE6A4
23CFF2F6630A2646AE45054EE34E87C7CD49A3162B40A0F7C5FD577D60C78135BCA117
F4522001F1A49748DA2E335F02EE12011ED86C64297E59D1AA866EF9A66CE994299C0C
48C83F25A086D767DCAB5A817B9F2C4AB5EAFE0A523F1CBAD1BD5C4C95F26C0219974A
7BB8E122DEBC8BA6AB8DC0A386A40A4CCEF82EF5E94C71ECCEBF31974CCE1F9B8A4D2E
95FA33079E4E31DAD42751AB53152AE6CCBD25BE2F481C4EAC3C89B7AF80D6A5EBC42C
B1CEC1F9C88F1173FA952CBFC80017374C77EAFD1332185D75C9D7DC95595F95B4499D
0E9DF320C4DE97CF2469CCB9FE29F5D5DC44608E3F9B092F5E41E4AB465E1AC74FE4DD
98906A6635BF7EB291D33D0F8ADAF60A11FE6808A0F83ED143C0E574D3D8AB40B049B7
29C5C464E453687F0FDA03E3CB64D13F724520B9743C7EB63489E3A7A8CDA1A88E9FAB
598DBB3EE335824252E10FC17CCAD1716555580595AE6DB41FD1259CE200849786E166
970B6A0CBDA207FFB43E38FB82777DB1346BFDFECDE8D92A5484DF84F2B143F553E39C
F649EC6E0F4ADA47EC4C5B7826051CC211F71C8396C18C2C565EEAB4B2F7B589004F0A
3DE76AEC82DE011FB1EF66EFD762DF3BD4F8FAFA7059E2E9E9DCE6",
    "digest_type": "SM3",
    "enc_type": "SM4",
    "method": "ehc.ehealthcode.verify",
    "term_id": "3500000104341",
    "timestamp": "1545921142502",
    "version": "1.0.0"
```

```
}
```

组成的**待签名字符串**为：

```
app_id=vzusug4lhvq2enpxer&biz_content=E1A78A21826D512E685B599A960D7E417493315542ABB76EF85A73EF2351AEF120528E31E8EE4344FE644FD30349271F32CC6926188815B37177527C0F78722DCC85CAD4D959176E6A315173DBB9072FC0AB9359485AA6F2F905ACBD3BAD93300A43B5E9F39C3C0025B91F7CBAC3F80C49B5E2DE39BF43654C67FBF0B2094EE6A423CFF2F6630A2646AE45054EE34E87C7CD49A3162B40A0F7C5FD577D60C78135BCA117F4522001F1A49748DA2E335F02EE12011ED86C64297E59D1AA866EF9A66CE994299C0C48C83F25A086D767DCAB5A817B9F2C4AB5EAFE0A523F1CBAD1BD5C4C95F26C0219974A7BB8E122DEBC8BA6AB8DC0A386A40A4CCEF82EF5E94C71ECCEBF31974CCE1F9B8A4D2E95FA33079E4E31DAD42751AB53152AE6CCBD25BE2F481C4EAC3C89B7AF80D6A5EBC42CB1CEC1F9C88F1173FA952CBFC80017374C77EAFD1332185D75C9D7DC95595F95B4499D0E9DF320C4DE97CF2469CCB9FE29F5D5DC44608E3F9B092F5E41E4AB465E1AC74FE4DD98906A6635BF7EB291D33D0F8ADAF60A11FE6808A0F83ED143C0E574D3D8AB40B049B729C5C464E453687F0FDA03E3CB64D13F724520B9743C7EB63489E3A7A8CDA1A88E9FAB598DBB3EE335824252E10FC17CCAD1716555580595AE6DB41FD1259CE200849786E166970B6A0CBDA207FFB43E38FB82777DB1346BFDFECDE8D92A5484DF84F2B143F553E39CF649EC6E0F4ADA47EC4C5B7826051CC211F71C8396C18C2C565EEAB4B2F7B589004F0A3DE76AEC82DE011FB1EF66EFD762DF3BD4F8FAFA7059E2E9E9DCE6&digest_type=SM3&enc_type=SM4&method=ehc.ehealthcode.verify&term_id=3500000104341&timestamp=1545921142502&version=1.0.0&app_secret=BEE975CC71E21F3FE87DE9F7121DE31F09B93D1AC804A60BBF877C240EBB0FC6
```

4. 签名结果

使用各自语言对应的 SM3 签名函数，对拼接商户私钥得出的待签名字符串进行 SM3 签名后，再将字节码转换成 16 进制字符串，并对转换后的字符串转换成大写，即是签

名结果，如：

851C041BC8D788CDA5B87CAD96451A90BD2C8F81BA07F2A6954F69FC3D3BB2A6

3.4.2.2 返回报文-摘要值验证流程

（与请求签名类似）

1. 筛选

获取所有请求参数，不包括字节类型参数，如文件、字节流，并剔除 digest 字段。

2. 排序

将筛选的参数按照第一个字符的键值 ASCII 码递增排序（字母升序排序），如果遇到相同字符则按照第二个字符的键值 ASCII 码递增排序，以此类推。

3. 拼接

将排序后的参数与其对应值，组合成“参数=参数值”的格式，并且把这些参数用&字符连接起来，最后拼接上应用密钥 app_secret，格式如下

“…参数=参数值&app_secret=你的密钥”

此时生成的字符串为待签名字符串，对待签名字符串 SM3 运算，即是摘要（digest）的值。

注意：“DIGEST”参数不参与签名

例如下面的请求示例，参数值都是示例，开发者参考格式即可：

如请求的返回内容为：

```
{
    "app_id": "vzusug4lhvq2enpxer",
    "biz_content":
"1F61C3BC533DCD0E174EBC7A6D18A18BF6F21C29476DF75976D72068D3B720903FE
5FEE28471811A42D59347761868C14E93E9FAED5FB54434CB2C47163E01B5981CA46
```

5A4E1D9C3BE1861DBA53F02A34E08204333866CD772510BBF1BC0DFDCF4376C1278C
00C004EE8266650DDB82D59AAA416F4FF71B8A0A7C52E1469341F4677B0079C1ABB0
DCE49B6C61AC4D25505B10EE25B9D6AF94E69E14938DABE2D408949F60535D805758
A21D77AA6FA5420596C0091650F3D16AEAF2B416DD5E1CB541DFD0A30451751D965C
CC34007BF82A320C840A8EAB67E42E62B912812A703CFFD76888A933B669B8B55FC9
F00E0AD0E1499AC29BD506C05ED24A4BF3DBA73470E0AB125B6368373B07CF1C24B3
AFDF55C0C274D437795BA74D351382E535869844FCDE9A44A738F40C4FBB9B91BAF8
168FAE61478BAD53BF1FE1CE03B3E0CAFA52147F51EE8EA9A465AB005A6A33C98E69
3CB431241610739270BC58186FCAC6AEC6FD14BA8D0339255747CA18599420532A34
D3D1E6C8C36D79EC3BC6675056A3D32F300B6B3735F2C1614543B7CB1CD2454D28EE
53891546DF3B5EDFBFDC1DB9D2F9E4CB19A403E1F71B72D410EB0D84390C73BAC35B
51BE2C74F79565169BD8F3D911DC81CDD12EA81DD30A6775C838036059060ACCAF35
F7A8125E0853DC13DCA82ACFC09507A50A1D3955B21FE03A687CF07B3F9512A21DE5
97354E564B2619982E2A335D804A02CABBE3821FE03A687CF07B3F9512A21DE59735
405CAFD378552C9F5133866260989C7708A4C347E99FB218A5E0A0040492094A0356
0C560AB6033FAFCFFD3BA048FB745B40C252870E9043742D3B33F8FF3C70AA9A8772
CE50131D777BF300D02BC20E189883F46A308B7E08FD5C150CA094486FEDE6DC064A
C9D5D92B65BA34786D0FECC4C6F75985618C6D792ABD53CF54F2E80DF8C1C5B6EEFF
975D5FFF04E5CB831213A60ECBEDD7A2BEF26C491CA6C7E436C71C24AFA20D6F31A9
E4AD2337E2A39B16B50EC54343A6F18261DC06B8C088F94EC15F25308AFE5686FDDE
33E51F6268666E7134F896EB5CCC4A60D77789FAA819E6CA2FA063E099B1FE0EF32E
369A1D2C59F2FD7EA1262DFF01D532C68971B94EC15F25308AFE5686FDDE33E51F62
68666E7134F896EB5CCC4A60D77789FAAFB85DD60057073B927DBE2BACE6B0B6EB5F
F5E3D517A24D35938EADD36E6BC5EAE5B325A1C968335AC1C68CAC477B9688B9AE08
CE4604C082111B2E5B380E4B6208D1B304BA36D992A333F8D3D78FB0D0FF831C4CE3
502372CFE5DD975879AFAF986875DC698BE17B11A09E9C938D1008D88F00F0E5E652
870CC432F6AD23234EE11BD71653AAD237AC7521D59D94E68FD3742537BB24866031
CE7A62E4AD327BE171E91185A868AF3D5F443FEB5E346EE6482FFC85A60B16F7FEB0

```
C9D69FA29E47EF474157BC6FC51C17E77DF17B06C2FD5BA71C54A52E1C8BB9DF3353
291C00224A38DE871C028AD0689C6BF34E2B29D526504C89C0F9E47E81F818B44A76
5D9EA44AA0FB5FDD6B115C80EEDF4EB5D5EE4BE22176E00A70531075E11B083D9005
3BF0B35B10845E99CACB9EBD390F9694CC8DD37F7FBFB82048DF3AB97B306873B7C8
9045F88D5219BB008FC7B766DB4FB91CBD2AA07CD63EFF61AF3602F83BF6D5E56A3F
91ACC574CD80ADE0C847801B561179DB87BB024494E7A747C1E69AB01CC52ED382BB
CA39D0A5894D978A8BE06863AA322855247E136C6BDD8DD3549DAA0DC4256449A5C1
3887241386EAC94CE8F0DAA7AE5D5777BF41BFBB74AD7",
      "digest":
"45D8681184A414B406D52C4E45B38BA5D44ED2F072F85D4F3EDA8C92028E480B",
      "digest_type": "SM3",
      "enc_type": "SM4",
      "method": "ehc.ehealthcode.verify",
      "ret_code": "0000",
      "ret_msg": "交易成功",
      "sign": "",
      "sign_type": "",
      "timestamp": "20181227223223",
      "version": "1.0.0"
   }
```

则待验签内容为：

```
   app_id=vzusug4lhvq2enpxer&biz_content=1F61C3BC533DCD0E174EBC7A6D
18A18BF6F21C29476DF75976D72068D3B720903FE5FEE28471811A42D5934776186
8C14E93E9FAED5FB54434CB2C47163E01B5981CA465A4E1D9C3BE1861DBA53F02A3
4E08204333866CD772510BBF1BC0DFDCF4376C1278C00C004EE8266650DDB82D59A
AA416F4FF71B8A0A7C52E1469341F4677B0079C1ABB0DCE49B6C61AC4D25505B10E
```

E25B9D6AF94E69E14938DABE2D408949F60535D805758A21D77AA6FA5420596C009
1650F3D16AEAF2B416DD5E1CB541DFD0A30451751D965CCC34007BF82A320C840A8
EAB67E42E62B912812A703CFFD76888A933B669B8B55FC9F00E0AD0E1499AC29BD5
06C05ED24A4BF3DBA73470E0AB125B6368373B07CF1C24B3AFDF55C0C274D437795
BA74D351382E535869844FCDE9A44A738F40C4FBB9B91BAF8168FAE61478BAD53BF
1FE1CE03B3E0CAFA52147F51EE8EA9A465AB005A6A33C98E693CB43124161073927
0BC58186FCAC6AEC6FD14BA8D0339255747CA18599420532A34D3D1E6C8C36D79EC
3BC6675056A3D32F300B6B3735F2C1614543B7CB1CD2454D28EE53891546DF3B5ED
FBFDC1DB9D2F9E4CB19A403E1F71B72D410EB0D84390C73BAC35B51BE2C74F79565
169BD8F3D911DC81CDD12EA81DD30A6775C838036059060ACCAF35F7A8125E0853D
C13DCA82ACFC09507A50A1D3955B21FE03A687CF07B3F9512A21DE597354E564B26
19982E2A335D804A02CABBE3821FE03A687CF07B3F9512A21DE59735405CAFD3785
52C9F5133866260989C7708A4C347E99FB218A5E0A0040492094A03560C560AB603
3FAFCFFD3BA048FB745B40C252870E9043742D3B33F8FF3C70AA9A8772CE50131D7
77BF300D02BC20E189883F46A308B7E08FD5C150CA094486FEDE6DC064AC9D5D92B
65BA34786D0FECC4C6F75985618C6D792ABD53CF54F2E80DF8C1C5B6EEFF975D5FF
F04E5CB831213A60ECBEDD7A2BEF26C491CA6C7E436C71C24AFA20D6F31A9E4AD23
37E2A39B16B50EC54343A6F18261DC06B8C088F94EC15F25308AFE5686FDDE33E51
F6268666E7134F896EB5CCC4A60D77789FAA819E6CA2FA063E099B1FE0EF32E369A
1D2C59F2FD7EA1262DFF01D532C68971B94EC15F25308AFE5686FDDE33E51F62686
66E7134F896EB5CCC4A60D77789FAAFB85DD60057073B927DBE2BACE6B0B6EB5FF5
E3D517A24D35938EADD36E6BC5EAE5B325A1C968335AC1C68CAC477B9688B9AE08C
E4604C082111B2E5B380E4B6208D1B304BA36D992A333F8D3D78FB0D0FF831C4CE3
502372CFE5DD975879AFAF986875DC698BE17B11A09E9C938D1008D88F00F0E5E65
2870CC432F6AD23234EE11BD71653AAD237AC7521D59D94E68FD3742537BB248660
31CE7A62E4AD327BE171E91185A868AF3D5F443FEB5E346EE6482FFC85A60B16F7F
EB0C9D69FA29E47EF474157BC6FC51C17E77DF17B06C2FD5BA71C54A52E1C8BB9DF
3353291C00224A38DE871C028AD0689C6BF34E2B29D526504C89C0F9E47E81F818B

	44A765D9EA44AA0FB5FDD6B115C80EEDF4EB5D5EE4BE22176E00A70531075E11B083D90053BF0B35B10845E99CACB9EBD390F9694CC8DD37F7FBFB82048DF3AB97B306873B7C89045F88D5219BB008FC7B766DB4FB91CBD2AA07CD63EFF61AF3602F83BF6D5E56A3F91ACC574CD80ADE0C847801B561179DB87BB024494E7A747C1E69AB01CC52ED382BBCA39D0A5894D978A8BE06863AA322855247E136C6BDD8DD3549DAA0DC4256449A5C13887241386EAC94CE8F0DAA7AE5D5777BF41BFBB74AD7&digest_type=SM3&enc_type=SM4&method=ehc.ehealthcode.verify&ret_code=0000&ret_msg=交易成功&timestamp=20181227223223&version=1.0.0&app_secret=BEE975CC71E21F3FE87DE9F7121DE31F09B93D1AC804A60BBF877C240EBB0FC6

4. 签名结果

对待验签内容 SM3 后，将字节码转换成 16 进制字符串，并对转换后的字符串转换成大写，即是签名结果

如：45D8681184A414B406D52C4E45B38BA5D44ED2F072F85D4F3EDA8C92028E480B

再与返回报文里的 digest 字段比较是否匹配，根据比较结果判定是否验签通过。

4 接口规范

4.1 卡管登记注册接口

本接口用于电子健康卡管理系统通过跨域认证服务登记接入电子健康卡管理信息系统的系统相关信息。

接口地址	跨域认证服务节点
接口方法	ehn.ehealthmanage.register
接口描述	电子健康卡管理信息系统通过跨域认证服务注册或变更接入电子健康卡联网
接口使用	电子健康卡管理信息系统在接入全国联网时，如果未注册需要调用该接口注册电子健康

	卡管理系统信息，如果已注册有变更也需要调用进行变更。
接口提供者	跨域认证服务
主要使用者	电子健康卡管理信息系统

请求消息：

示例


```
{
"ehcnet_app_id":"vzusug4lhvq2enpxer",
"biz_content":" {\"ehcnet_url\":\"***\",\"ehc_in\":\"{***}\"} ",
"digest_type":"SM3",
"enc_type":"SM4",
"method":"ehn.ehealthmanage.register ",
"term_id":"3500000104341",
"timestamp":"1563787684851",
"version":"1.0.0"
}
```


名称	说明	数据类型及长度	备注
method	接口名称	String(50)	
app_id	应用编号	String(32)	
term_id	终端编号	String(32)	
version	接口版本号	String(10)	
timestamp	请求时间戳	String(20)	
digest_type	摘要类型	String(10)	
digest	摘要内容	String(256)	
enc_type	加密类型	String(10)	
biz_content	请求参数集合	String(-)	
<< biz_content 接口请求参数>>			

ehcnet_url	联网接入地址	String(64)	
ehcnet_app_id	联网接入应用编号	String(64)	
ehcnet_app_secret	联网接入应用密钥	String(64)	
ehc_in	卡管节点入网编码	String(32)	9 位卡管节点入网编码 3502A0001

应答消息：

示例


```
{
"echnet_app_id":"vzusug4lhvq2enpxer",
"biz_content":"",
"enc_type":"SM4",
"method":"ehn.ehealthmanage.register",
"ret_code":"0000",
"ret_msg":"交易成功",
"digest":"***",
"digest_type":"SM3",
"timestamp":"20190722170739",
"version":"1.0.0"
}
```


名称	说明	数据类型及长度	备注
ret_code	返回结果码	String(10)	
ret_msg	返回结果说明	String(200)	
app_id	应用编号	String(20)	
method	接口名称	String(50)	

version	接口版本号	String(10)	
timestamp	响应报文时间戳	String(20)	
digest_type	摘要类型	String(10)	
digest	摘要内容	String(256)	
enc_type	加密类型	String(10)	

4.2 电子健康卡跨域认证接口

本接口用于电子健康卡跨域验证二维码并返回验证结果信息。

接口地址	跨域认证服务接口地址、电子健康卡管理信息系统联网地址
接口方法	ehn.ehealthcard.syncCheckErhcInfo
接口描述	电子健康卡管理信息系统通过跨域认证服务申请验证非本卡管注册的电子健康卡二维码验证信息，跨域认证服务将路由至对应发卡机构进行验证后返回电子健康卡及居民信息；跨域认证服务向发卡机构提交验证电子健康卡二维码请求，如果验证成功，返回电子健康卡及居民信息。
接口提供者	跨域认证服务、电子健康卡管理信息系统
主要使用者	电子健康卡管理信息系统、跨域认证服务

请求消息：

示例


```
{
"app_id":"vzusug4lhvq2enpxer",
"biz_content":"{\"operator_name\":\"医生
\",\"ehealth_code\":\"***\",\"treatment_code\":\"010101\",\"operator_id\":\"001\",\"ou
t_verify_time\":\"20190722165036\",\"out_verify_no\":\"ad394583a0594a58b91f8d32a228db6
2\"}",
```

```
"digest_type":"SM3",
"digest":"***",
"enc_type":"SM4",
"method":"ehn.ehealthcard.syncCheckErhcInfo",
"term_id":"1100000104341",
"timestamp":"1563785437006",
"version":"1.0.0"
}
```

名称	说明	数据类型及长度	备注
method	接口名称	String(50)	
app_id	应用编号	String(32)	
term_id	终端编号	String(32)	
version	接口版本号	String(10)	
timestamp	请求时间戳	String(20)	
digest_type	摘要类型	String(10)	
digest	摘要内容	String(256)	
enc_type	加密类型	String(10)	
biz_content	请求参数集合	String(-)	
<< biz_content 接口请求参数>>			
out_verify_no	外部验证发起流水号	String(32)	
out_verify_time	外部验证发起时间	String(32)	
ehealth_code	待验证的电子健康卡二维码	String(128)	
treatment_code	诊疗环节编码	String(32)	详见材料一附录 E 编码定义

应答消息：

示例

{
"app_id":"vzusug4lhvq2enpxer",
"biz_content":"{\"birthday\":\"19901102\",\"ehealth_card_id\":\"***\",\"address\":\"\"
,\"user_name\":\"***\",\"telephone\":\"\",\"card_type\":\"01\",\"mindex_id\":\"***\",\"use
r_sex\":\"1\",\"work_unit\":\"\",\"id_no\":\"***\" ,\"mobile_phone\":\"***\",\"id_type\":\
"01\"}",
"enc_type":"SM4",
"method":"ehn.ehealthcard.syncCheckErhcInfo",
"ret_code":"0000",
"ret_msg":"交易成功",
"digest":"***",
"digest_type":"SM3",
"timestamp":"20190722170739",
"version":"1.0.0"
}

名称	说明	数据类型及长度	备注
ret_code	返回结果码	String(10)	
ret_msg	返回结果说明	String(200)	
app_id	应用编号	String(20)	
method	接口名称	String(50)	
version	接口版本号	String(10)	
timestamp	响应报文时间戳	String(20)	
digest_type	摘要类型	String(10)	
digest	摘要内容	String(256)	
enc_type	加密类型	String(10)	

biz_content	接口返回参数	JSONString	
<< biz_content 接口返回参数>>			
issuer_org_name	发卡机构名称	String(32)	
issuer_org_code	发卡机构代码	String(32)	
issuer_province_code	发卡省份行政区划代码	String(32)	
issuer_city_code	发卡城市行政区划代码	String(32)	
id_type	证件类型	String(2)	
id_no	证件号	String(32)	
user_name	用户姓名	String(50)	
user_sex	用户性别	String(1)	
mobile_phone	手机号码	String(32)	
birthday	出生日期	String(10)	
nation	民族	String(50)	
telephone	联系电话	String(32)	
address	居住地址	String(200)	
work_unit	工作单位	String(100)	
citizen	国籍	String(2)	
career	职业	String(3)	
unit_phone	单位电话	String(20)	
email	邮箱	String(120)	
ehealth_card_id	健康卡 ID	String(128)	
mindex_id	主索引 ID	String(128)	

5 返回码说明

返回码	返回码描述	解决方案
0000	操作成功	
9998	交易失败	
9999	未知错误	
1001	应用编号为空	

1002	终端编号为空	
1003	不支持交易版本号	
1004	接口名称不为空	
1005	接口名称不合法	
1006	未知加密类型	
1007	未知签名类型	
1008	应用不存在	
1009	终端不存在	
1010	应用无该接口权限	
2001	电子健康卡二维码已过期	
2002	电子健康卡二维码不合法	
2003	有效时间为空	
2004	有效时间不合法	
2005	密码服务失败	
3001	无符合条件的查询记录	
3002	流水号重复	
3003	资源正在被占用，请确认交易状态再试	
8001	网络读失败	
8002	网络传输出错	
8003	空网络请求	
8004	网络连接失败	
8005	数据库连接失败	
8006	数据库配置加载失败	
8007	数据操作失败	
8008	密码服务失败	
8009	内部异常	
9001	请求参数有误	
9002	签名失败	
9003	验签失败	
9004	响应报文为空	
9005	请求系统不支持	
9006	报文加密失败	
9007	报文解密失败	
9008	报文读取错误	

6 字典说明

详细请参考材料一附录E：国家电子健康卡应用监测系统数据采集标准规范-7.字典定义