合同书

甲方：北京市民政局

乙方：北京农村商业银行股份有限公司与北京市政交通一卡通支付有限公司联合体

甲、乙双方依据《中华人民共和国民法典》等相关法律法规的规定，遵循平等、自愿、有偿的原则，经协商一致，签订本合同。

第一条 定义

本合同中的下列术语应解释为：

1.1 “合同”系指双方签署的、合同格式中载明的甲乙双方所达成的协议，包括所有的附件、附录和构成合同的其它文件。

1.2 “合同总价”系指根据合同约定，乙方在完全履行合同义务后甲方应付给乙方的价格。

1.3“卡片”必须符合《北京市社会服务一卡通（北京通）卡片技术规范》（DB11/T 1179-2015）（详见附件 3）标准及市政交通一卡通标准。

1.4“服务”系指根据合同约定乙方承担与本项目有关的所有服务。

1.5“甲方”系指与成交人签署合同的单位。

1.6“乙方”系指根据合同约定提供相关服务的成交人。

1.7“验收”系指合同双方依据强制性的国家技术质量规范和合同约定，确认合同项下的服务符合合同规定的活动。

第二条 服务内容

在全市“多卡合一”实行前，甲方作为卡的发行主体，负责卡的发行、运营及管理工作。

乙方负责养老助残卡的具体申办受理、制发等工作，按甲方要求为符合条件的发放对象制发卡、受理卡的相关业务。发放卡的数量不低于 525482 张。

2.1 乙方服务内容包括但不限于单一来源采购文件及被甲方接受的响应文件及响应承诺中的约定。

2.2 卡的功能

2.2.1 优待功能。北京通-养老助残卡用户可享受符合《北京通—养老助残卡管理办法》

京民老龄发〔2018〕418号第八条要求（详见合同附件）等北京市老年人优待政策规定的优待服务。

2.2.2 借记功能。北京通—养老助残卡具备银行借记卡功能。借记卡功能激活及使用参照乙方相关规定执行。

2.2.3 政策性功能。北京通-养老助残卡用户可享受符合《北京通—养老助残卡管理办法》京民老龄发〔2018〕418号第十条要求（详见合同附件）等相关养老服务政策规定的政策性服务。并根据政府养老服务相关政策体系发展需要，不断扩展政策性功能，如养老服务补贴津贴发放等。

2.2.4 满足甲方对卡政策实施的其它要求。

2.3 乙方负责对现有北京通养老助残卡管理系统改造升级，以满足甲方业务及卡片的受理要求，保证卡片的售后服务标准不低于《北京市社会服务一卡通（北京通）卡片技术规范》（DB11/T 1179-2015）要求。

2.4 乙方同意甲方为卡发行主体，甲方提供其政策相关的业务规范，乙方按照甲方要求进行卡片的发行、银行卡部分的运营及管理。

2.5 卡的制作与管理

2.5.1 乙方负责按照甲方的账户设置、功能要求、卡面要求等进行卡片的制作与管理、具备市政交通一卡通功能，满足老年人优待服务的准确实施。

2.5.2 乙方应承担的制卡成本，包括卡片制作、芯片采购、卡套设计及采购、卡绳采购及其他费用，乙方应全部完成制卡、发放及保障服务工作。乙方完成卡片初始化业务、技术应用保障业务和延期等相关一卡通业务的衔接与办理，保障一卡通功能的有效实施、信息准确完整。

2.5.3 乙方负责卡片的申办受理、开卡、发放、卡内养老政策性津贴额度的划拨、结算以及后期服务（挂失、补卡、换卡、激活、延期、注销、移资、客服咨询、上门服务、数据安全保障）工作。

2.5.4 乙方需制定卡的申请服务方案。乙方接受老年人申请后，现场初审申请人的身份、户籍及年龄条件，并于24小时内将初审通过的申请信息上报甲方指定审核方进行资质审核，审核通过后进入制卡流程，制卡时限自申请之日起不超过20天，制卡完成后网点通过短信或电话的方式通知客户领卡。

2.5.5 临时卡发放要求

2.5.5.1 临时卡的发放标准

若出现申请人卡片丢失、卡片人为损坏，乙方可根据申请人的申请提供临时卡并收取成本费及一卡通初始费；符合领卡资格但未到领卡时间的申请人如要求享受公交、公园优待的情况，乙方可向申请人提供临时卡并收取成本费及一卡通初始费；临时卡的成本费及一卡通初始费按本合同 5.1 条款标准收取。若出现制卡失败、卡片非人为损坏（卡面完整，无人为损坏痕迹即视为非人为损坏）等原因导致申请人未能及时领用养老助残卡，乙方需免费为申请人提供临时卡。

2.5.5.2 临时卡的成本及承担方

免费临时卡的成本按本合同 5.1 条款标准、按责承担，其中因乙方原因造成制卡失败产生的临时卡成本由乙方承担；因卡片非人为损坏造成的临时卡成本，如因生产过程中制造工艺产生的质量问题，由乙方承担；因特殊情况由甲方指定人审核后发放的临时卡，其成本按本合同 5.1 条款标准由甲方向乙方支付费用。

2.5.5.3 临时卡的信息推送要求

乙方须于发卡当日内通过银行制卡系统向甲方推送临时卡数据，且按甲方要求对临时卡进行管理。临时卡由乙方负责制发与管理并给予临时卡发行技术支持，乙方需规范卡的发行、使用与回收，接受甲方的监督与审查。乙方须在发卡时将临时卡相关规定告知申请人，申请人接受后方可领用。

2.5.5.4 临时卡的有效期及其他要求

临时卡有效期自领用之日起为两个月，不可延期、过期失效，卡片具有公交、公园免费刷卡功能，卡片采用实名制领取，乙方须核实老年人身份。老年人如丢失临时卡不能办理解挂业务。

2.5.6 乙方按照甲方下达的制卡、发卡通知按时完成发卡工作，并将制卡结果数据于制卡完成后 T+1 日反馈甲方，供甲方随时查询制卡过程中的步骤。乙方同时应为持卡人及商户提供卡片及养老（助残）便民服务商提供绿色服务通道。

2.5.7 乙方负责按照甲方对于卡片功能的要求，在卡片中整合市政交通一卡通功能。

2.5.8 甲方负责建立养老助残卡有效卡数据库，持卡人至乙方处申请延期，乙方通过系统查询有效卡数据库，符合继续使用标准的予以延期，不符合使用标准的不得延期。

2.5.9 乙方要按照甲方要求和发卡时限将卡片发放给老人，并提供专门针对老年人的发卡与后期服务方案及时限。发卡的同时配发卡的使用手册和统一的卡套和卡绳，并告知当事人关于收费、激活、延期、挂失、补办等卡使用与管理的重要事项，卡套和卡绳样式需与甲方协商确认。

2.5.10 乙方受理老年人养老助残卡挂失、补办业务时，乙方网点操作员需核实申请人有效身份证件；如本人不能办理，代办人还须持代办人身份证件办理。换卡制卡周期同新卡，制卡完成后乙方通知申请人或代办人到办理挂失业务的网点领取。

2.5.11 乙方受理养老助残卡换损、移资（一卡通电子钱包）业务时，网点操作员需核实有效证件；如本人不能办理，代办人还须持代办人身份证件办理。网点操作员回收损坏卡片，并为用户申请办理新的养老助残卡，制卡周期同新卡，制卡完成后乙方通知申请人到前期办理换损、移资（一卡通电子钱包）业务的乙方网点领取。除因持卡人责任原因导致的卡片损坏由持卡人承担换卡成本外，其它由卡片技术原因导致的卡片损坏，根据卡片损坏原因，由乙方承担，报甲方备案。

2.5.12 乙方须对卡产生的所有金融业务数据、交通、公园业务数据进行运维管理，依法保障数据的使用安全。

2.5.13 乙方须保留完整准确的业务数据，信息系统按要求进行数据交换，数据交换内容与格式由甲方按业务需求审核确认与管理，保障数据安全。

2.6 网点设置

2.6.1 乙方网点服务范围能全覆盖北京市所有区，全市范围内营业网点数量不低于 300 家，郊区营业网点数量不低于 200 家，全市范围内人工受理业务网点数量不低于 200 家，全市范围内 ATM 机数量不低于 500 台，并在现有营业网点无法覆盖区域增设临时服务站点，乙方须提供详细的服务网点及临时服务站点名单。

2.6.2 乙方对各区、各街道乡镇实现服务对接，根据老年人需求不定期组织集中业务办理服务。对于因行动不便等原因导致老年人无法到乙方网点申请的情况，应根据用户需求安排当地网点工作人员或派专人提供上门服务，免收服务费。

乙方需在合同生效后向甲方提供对接服务网点情况、服务方案、联系方式等信息，并按要求向各区提供服务。

2.7 运行平台相关

2.7.1 北京通卡业务平台。具备发放北京通卡片的业务平台，可以满足业务发卡需求。

2.7.2 信息安全管理方案。乙方提供可行的信息安全管理方案，保证项目中所涉及的业务信息安全。

2.7.3 乙方平台系统升级或维护影响相关业务时，须提前两个工作日以书面形式通知甲方，尽量安排在不影响用户使用的时间，遇乙方平台系统出现故障，将具体受影响业务名称及恢复时间立即以传真形式通知甲方，如重大故障需延长修复时间，须告知甲方预计维修时间。

2.8 服务支撑

2.8.1 乙方负责依托自身具有的 APP 或其微信公众号等电子渠道支持服务。

2.8.2 客服服务。乙方开通办理业务绿色通道，开通 24 小时热线服务电话：96198，针对持卡老年人按甲方要求提供相关政策咨询服务。咨询服务内容包含卡的所有业务，在官网上提供政策咨询、业务查询与信息公开，同时开展相应的线下保障服务（包括制卡进度查询、补换卡、提供临时卡等）。乙方应根据甲方政策调整，做好服务机构培训，确保服务人员及时准确熟悉掌握养老助残卡制发卡等相关政策变化及对外解答口径，加强对银行电话客服人员的培训，提高服务的专业性和规范性，并制定机制年底进行考核，答复满意率需达到 90%及以上。

2.8.3 为保证项目中卡的受理点覆盖率，方便持卡人及养老（助残）服务单位办理各项银行业务，乙方负责对接社区，提供包括申请、制卡、领卡或使用咨询等服务，并为行动不便的老年人提供上门服务。乙方负责开发养老助残卡相关功能的银行电子受理渠道。

2.9 为保证资金的安全，乙方负责对卡在使用过程中发生的金融事故进行处理，保障卡的金融安全。对卡制发过程中可能出现的风险进行防控与化解，处理责任事故。

2.10 乙方提供的金融服务如银行卡借记功能等内容必须遵守中国人民银行、中国银保监会等乙方监管机构政策规范。

2.11 卡片初始化与一卡通功能技术保障服务

乙方需为北京通-养老助残卡实现一卡通功能提供卡片初始化服务，并同时提供以下

服务：

2.11.1 乙方为北京通-养老助残卡提供一卡通应用，包括卡片初始化、公交公园免费刷卡应用、其他一卡通交通行业应用（包括但不限于轨道交通）、以及一卡通延期/换损/移资/退资等业务。

2.11.2 养老助残卡为实名制一卡通卡，在后台系统采用实名制管理，乙方须获取用户实名信息后方可进行卡片个人化，实名信息应包含但不限于如下内容：姓名、身份证号、手机号、性别、家庭住址、出生日期、一卡通卡号、北京通号、银行卡号等。有效期设置为两年，有效期内 60 周岁及以上老人持卡在公交、公园可免费刷卡乘坐，在其他一卡通应用领域可使用电子钱包支付，如：轨道交通等。

2.11.3 乙方卡片须保障北京通-养老助残卡的制作数量，并按照甲方工作进度要求完成批量制卡工作。

2.11.4 养老助残卡过期后可到乙方指定网点或商户办理延期，采用联机模式，已注销（去世）、挂失、换损卡将不再提供延期；电子钱包内有余额的，由乙方受理移资业务。乙方对已损坏的卡片进行技术处理并进行回收。

2.11.5 乙方系统每日与市社会福利服务管理平台等系统进行交互数据。

2.11.6 公园和公交刷卡机具有落实持卡人免费乘公交、免费或优惠逛公园等政府优待政策的功能，为了保证政府优待政策的高效，提升持卡人用户体验度，乙方须对具备甲方设备的公园和公交刷卡机及所在场所的优待政策执行情况进行维护、在五一，十一，春节假日前进行抽检，并根据需求变化进行系统升级，保障老年卡在公园和公交场所的正常刷卡功能。

2.11.7 乙方“养老助残卡实名管理信息系统”平台为每个养老助残卡持卡人建立后台实名管理信息账户，用于持卡人实名信息及状态管理维护建立养老助残前置系统，用于实现专用 POS 机及甲方指定系统的接入。一卡通联机系统支持养老助残卡联机业务的后台处理，如：延期、换损、移资、挂失、解挂等，延期业务后台自动审核持卡人状态功能，通过访问“养老助残卡实名管理信息系统”获取持卡人的最新状态，对于已注销、挂失、换损的卡片不再提供延期功能。乙方后台系统与甲方指定系统之间采用专线连接，甲方指定系统实时或定期向乙方系统发送持卡人制卡信息、注销信息、挂失信息、变更信息等，用于养老助残卡的制卡、实名信息维护、状态变

更、延期等业务。

2.11.8 专用 POS 机

乙方网点办理养老助残卡的一卡通相关业务，通过一卡通专用 POS 机办理。一卡通专用 POS 机的业务功能主要包括：一卡通应用延期、换损移资、脱机查询、电子钱包充值/圈存、电子钱包消费等。

2.11.9 卡片延期：乙方按甲方要求在指定网点 POS 机上进行延期。

2.11.10 卡片注销：乙方按甲方要求对不符合条件卡进行注销标记，对已销户的卡片后台做如下限制：（1）将不再对卡进行延期、（2）已过期的卡电子钱包不允许充值但可退资（有效期内的卡仍可充值）。

2.11.11 数据管理：乙方对市政一卡通领域产生的应用数据进行运维管理，保障数据的使用安全。按甲方要求定时将养老助残卡有效数据上报甲方指定业务系统。

2.11.12 其它领域应用：乙方根据甲方实际的用卡需求，开发其它领域应用功能。

2.11.13 一卡通应用技术保障服务：乙方须对卡在市政交通一卡通领域发生的事故进行处理，保障卡的使用安全。对本业务领域向社会提供完整的业务咨询服务和线下保障服务，咨询服务内容包含卡的所有业务（包括但不限于卡的应用、刷卡问题、技术问题解答等），在官网上提供政策咨询、业务查询与信息公开。

2.12 卡的延期业务终端运维服务：乙方根据甲方需求拓展延期业务的自助受理渠道，开发网上延期和 APP 延期服务，并为业务系统提供技术支持与后期保障服务。

2.13.1 延期设备采用专用 POS 机，为老年人提供养老助残卡延期服务，除保证正常运行的基本功能外，业务需求包括以下内容：

2.13.1.1 养老助残卡一卡通查询功能，查询内容包括卡片有效期截止日期、一卡通电子钱包余额；

2.13.1.2 养老助残卡一卡通延期功能，可将养老助残卡一卡通有效期自延期之日起顺延两个自然年，符合延期条件的即可办理延期，次数不设限；

2.13.1.3 不提供养老助残卡临时卡延期功能；

2.13.1.4 只为卡片信息完整且有效的养老助残卡提供延期服务，不符合条件的老年人需到银行进行延期。

2.14 乙方负责对政策需求的养老电子券账户和护理补贴账户进行开设及管理，负责提

供“多卡合一”后养老电子券账户和护理补贴账户的技术支持，确保“多卡合一”后继续提供现有账户体系支撑。

第三条 各方权利义务

3.1 甲方的权利义务

3.1.1 甲方有权对乙方的工作进行监督和审核，如在监督或审核的过程中发现乙方工作有不当之处，甲方有权提出建议，甲乙双方协商后，乙方应采纳其中的不违反国家法律法规及政策要求的建议。甲方有权对乙方工作成果进行抽样检查，以检验其工作的真实性和合理性。

3.1.2 甲方负责制定养老助残卡申请及审批标准（详见合同附件 1），乙方需根据甲方标准对申请信息进行初审，初审通过的申请信息上报甲方进行资质审核，审核通过后进入制发卡流程。

3.1.3 项目数据的权属为甲方，对外使用时乙方必须征得甲方书面同意。

3.2 乙方的权利义务

3.2.1 乙方按照甲方要求，按照《北京市社会服务一卡通（北京通）卡片技术规范》（DB11/T 1179-2015）标准及市政交通一卡通标准制卡，完成卡片初始化服务及一卡通功能技术保障服务。

3.2.2 乙方按照甲方要求于本合同生效之日起至 2025 年 12 月 31 日完成不低于 525482 张养老助残卡正式卡的发放。卡的申请、发放工作须在甲方监督下由乙方完成。

3.2.3 乙方应随时接受甲方的监督检查；

3.2.4 乙方应保证提交的工作成果符合甲方建议以及本合同约定的要求；

3.2.5 甲方对乙方提交的卡片制作、卡片发放、卡绳卡套采购及商户服务费用预算、卡片的申请、制作、发放及商户服务工作方案以及工作成果等提出质疑或者要求乙方答复、改正时，乙方应在收到甲方质疑后 7 个工作日内给予书面解释或答复；

3.2.6 乙方有权根据项目进展及时调整项目实施方案，但须征得甲方书面同意后方可实行；

3.2.7 乙方自行负担因履行本合同产生的各项税费；

3.2.8 乙方应对甲方支付的费用进行核算，不得列支与本合同无关的费用；

3.2.9 乙方需按甲方要求提供本合同约定的各项服务，不能单方面终止提供该服务。

3.2.10 非正常故障是指由于不可控因素导致设备整体出现故障，例如设备进水、设备损毁等，但不包括设备丢失。非正常故障的一卡通专用 POS 机故障率在 5%以内，由乙方免费维修更换，超过 5%以外的故障整机的维修费用，由甲方另行支付。

3.2.11 乙方应将政府购买服务项目与自身业务进行区分，在资金使用、业务宣传等工作中，不得存在交叉的情况。

3.2.12 乙方须指派专人专岗专职统筹本项目工作，对接甲方工作需求，处理日常线上业务服务工作。（详见合同附件 2）。乙方服务人员因工作表现不佳难以达到项目要求，甲方有权要求乙方更换，乙方应在 5 个工作日内向甲方提交替换人员名单，更换人员以不影响甲方工作进度及工作质量为原则。

第四条 知识产权

4.1 乙方应保证甲方在使用本项目服务或其任何一部分时不受第三方提出的侵犯专利权、著作权、商标权和工业设计权等的起诉。如果任何第三方提出侵权指控，乙方须与第三方交涉并承担由此发生的一切责任、费用和甲方全部损失，以及甲方为反驳第三方的主张或向乙方主张权利所支付的各项费用，包括但不限于调查费、律师费、诉讼费等。

第五条 付款条件和服务期限

5.1 本合同总价为 604.3043 万元人民币，大写陆佰零肆万叁仟零肆拾叁元人民币。

服务内容	价格（万元）	备注
制发卡服务	251.705878	不低于 525482 万张，单价 4.79 元，制卡补贴
	352.598422	不低 525482 万张，单价 6.71 元，卡片初始化服务等相关服务
合计	604.3043	

除本合同确定款项外，乙方不再收取任何额外费用。对于甲方所支付的项目款，乙方应做到专款专用，乙方所有的项目支出，应做到专门记账，倒溯可查。

乙方收款账户：

（1）名称：北京农村商业银行股份有限公司

纳税人识别号：91110000801124847M

地址：北京市西城区月坛南街1号院2号楼北京农商银行

电话：010-89198662

开户银行：北京农商银行总行营业部

开户行账号：2003000103000000182

（2）名称：北京市政交通一卡通支付有限公司

纳税人识别号：91110000801145381H

地址：北京市东城区东直门外大街39号院2号航空服务楼726房间

电话：010-88087755

开户银行：中信银行股份有限公司北京北苑支行

开户行账号：7116310182600002259

5.2.1 本合同生效后北京农村商业银行股份有限公司应提供等额、合法税务发票，甲方收到发票后10个工作日内，拨付北京农村商业银行股份有限公司70%合同价款，即人民币 壹佰柒拾陆万壹仟玖佰肆拾壹元壹角伍分（小 写：1761941.15元）；剩余30%合同价款，北京农村商业银行股份有限公司完成全部服务后20个工作日内由甲方组织验收，经甲方书面验收合格后15个工作日内，由甲方向北京农村商业银行股份有限公司拨付，即人民币柒拾伍万伍仟壹佰壹拾柒元陆角叁分（小写：755117.63元），该价款从本合同总价中列支。甲方书面验收合格后，付款前，乙方应提供等额、合法税务发票，否则，甲方有权拒绝付款。甲方在向乙方支付款项时，如遇市财政局国库结账等特殊时期，具体支付时间将根据北京市财政局有关规定执行，不视为甲方违约，但甲方要及时书面通知乙方，待障碍消除后，立即恢复支付。乙方不得因此延迟、中止、暂停、终止提供服务。

5.2.2 本合同生效后北京市政交通一卡通支付有限公司应提供等额、合法税务发票，甲方收到发票后10个工作日内，拨付北京市政交通一卡通支付有限公司70%合同价款，即人民币贰佰肆拾陆万捌仟壹佰捌拾捌元玖角伍分（小 写：2468188.95元）；剩余30%

合同价款，乙方完成全部服务后 20 个工作日内由甲方组织验收，经甲方书面验收合格后 15 个工作日内，由甲方向北京市政交通一卡通支付有限公司拨付，即人民币壹佰零伍万柒仟柒佰玖拾伍元贰角柒分（小写：1057795.27 元），该价款从本合同总价中列支。甲方书面验收合格后，付款前，乙方应提供等额、合法税务发票，否则，甲方有权拒绝付款。甲方在向乙方支付款项时，如遇市财政局国库结账等特殊时期，具体支付时间将根据北京市财政局有关规定执行，不视为甲方违约，但甲方要及时书面通知乙方，待障碍消除后，立即恢复支付。乙方不得因此延迟、中止、暂停、终止提供服务。

甲方开票信息如下：

名称：北京市民政局

纳税人识别号：11110000000021039C

5.3 服务期限:自合同签订之日起至 2025 年 12 月 31 日。

第六条 服务资料

6.1 本合同项下服务资料将以下列方式交付：乙方接到甲方书面通知后 15 天之内，将完成服务或合同所需必要资料交付给甲方。

第七条 保密责任

7.1 乙方保证对在谈判、签订、执行本合同过程中所获悉的属于无法自公开渠道获得的文件及资料（包括国家秘密、商业秘密、工作秘密、工作计划、运营活动、工作数据、财务信息、技术信息、经营信息及其他有关信息等）予以保密。未经甲方书面同意，不得向任何第三方泄露该商业秘密或未公开工作信息的全部或部分内容。但法律、法规另有规定或双方另有约定的除外。

7.2 乙方保证对在服务过程中所获悉的有关卡使用人的个人信息予以保密。

7.3 乙方须对本业务领域产生的数据信息予以保密，未经甲方书面同意，不得以任何形式向任何单位或个人泄露相关信息，或将相关信息用于北京通-养老助残卡业务以外的其他用途，法律、法规另有规定或另有约定的除外。

乙方必须指定专人负责老年人数据的使用与管理（包括查看、下载、拷贝、销毁等），采用加密、防篡改等技术手段保证老年人数据的安全。乙方需明确联系人姓名、电话、邮箱等相关信息，及时更新。

乙方必须采用技术管理措施，对项目涉及老年人数据的使用痕迹（包括查看、下载、

拷贝、销毁等）进行数据审计，并及时、完整地保留痕迹记录。记录内容包括但不限于老年人数据的使用时间、使用人、使用方式、数据内容等。应确保因故需要追溯项目涉及老年人数据的使用情况时，能够准确提供相关记录。

7.4 如果对是否属于保密信息存在争议，则乙方应按保密信息进行处理，除非得到甲方的书面明确否认。

7.5 本保密条款长期有效，不因本合同解除或终止而终止。

第八条 延迟服务

8.1 在履行合同过程中，如果乙方遇到不能按时提供服务的情况，应及时以书面形式将不能按时提供服务的理由、预期延误时间通知甲方。甲方收到乙方通知后，认为其理由正当的，可酌情延长提供服务时间，并以书面方式告知乙方延长期限。

第九条 违约条款

9.1 如果乙方没有按照本合同规定的时间或方式提供服务，或提供的服务不符合甲方要求、建议或本合同约定，或违反本合同第七条保密责任的，甲方可要求乙方支付违约金，违约金为合同总价的 5%。同时，甲方有权解除本合同，乙方除承担违约金外，应当赔偿由此给甲方造成的全部经济损失，尚未支付的款项甲方有权不予支付。乙方由于没有履行自己的义务，造成乙方在履行合同时违约或合同无法继续履行时，乙方应承担由此而造成的全部经济损失。

9.2 在乙方的下列违约情况下，甲方可向乙方发出书面通知，部分或全部终止合同。同时保留向乙方追诉的权利。

9.2.1 乙方未能在合同规定的限期或甲方同意延长的限期内，提供全部或部分服务,按合同第 9.1 的规定可以解除合同的；

9.2.2 乙方未能履行合同规定的其它主要义务（本合同 3.2.1~3.2.12 款）的；

9.2.3 在本合同履行过程中有腐败和欺诈行为的。

9.2.3.1“腐败行为”和“欺诈行为”定义如下:

9.2.3.1.1“腐败行为”是指提供/给予/接受或索取任何有价值的东西来影响甲方在合同签订、履行过程中的行为。

9.2.3.1.2“欺诈行为”是指为了影响合同签订、履行过程，以谎报事实的方法，损害甲方的利益的行为。

9.3 乙方不得以任何理由将本合同项下的服务项目转包、分包给第三方承担。否则甲方有权解除本合同，乙方除应退还甲方已支付的全部服务费外，还应向甲方支付本合同总金额 20%的违约金。

第十条 不可抗力

10.1 如果双方中任何一方遭遇法律规定的不可抗力，致使合同履行受阻时，履行合同的期限应予延长，延长的期限应相当于不可抗力所影响的时间。

10.2 受事故影响的一方应在不可抗力的事故发生后尽快书面形式通知对方，并在事故发生后 7 天内，将有关部门出具的证明文件送达对方。

10.3 不可抗力使合同的某些内容有变更必要的，双方应通过协商在 7 日内达成进一步履行合同的协议，因不可抗力致使合同不能履行的，合同终止。

第十一条 税费

11.1 与本合同有关的一切税费均适用中华人民共和国法律的相关规定。

第十二条 合同争议的解决

12.1 甲乙双方在本合同履行过程中如有争议，应协商解决。如协商不成，可向甲方所在地人民法院起诉。

第十三条 破产终止合同

13.1 如果乙方破产导致合同无法履行时，甲方可以书面形式通知乙方，单方终止合同而不给乙方补偿。但甲方必须以书面形式告知同级政府采购监督管理部门。该合同的终止将不损害或不影响甲方已经采取或将要采取的任何行动或补救措施的权利。

第十四条 转让和分包

14.1 本政府采购合同不能转让。

14.2 本项目不允许分包。

第十五条 合同修改

15.1 合同各方都不得擅自变更本合同，但合同继续履行将损害国家和社会公共利益的除外。如必须对合同条款进行改动时，须各方共同签署书面文件，作为合同的补充，并报同级政府采购监督管理部门备案。

第十六条 通知

16.1 本合同任何一方给对方的通知，都应以书面形式发送，而对方也应以书面形式确

认并发送到对方明确的地址。

甲方信息：

联系人:艾老师联系电话:01055522086 联系邮箱:ailinbo@mzj.beijing.gov.cn

联系地址：北京市通州区留庄路 4 号院 2 号楼北京市民政局

乙方信息：

北京农村商业银行股份有限公司信息：

联系人：唐柯 联系电话：13801122016 联系邮箱：tangke@bjrcb.com

联系地址：北京市西城区月坛南街 1 号院 2 号楼北京农商银行

北京市政交通一卡通支付有限公司信息：

联系人:于鸿涛联系电话:13901215013 联系邮箱:yuhongtao@bmac.com.cn

联系地址：北京市东城区东直门外大街 39 号院 2 号航空服务楼 726 房间

第十七条 计量单位

17.1 除技术规范中另有规定外,计量单位均使用国家法定计量单位。

第十八条 适用法律

18.1 本合同应按照中华人民共和国的法律进行解释。

第十九条 合同生效和其它

19.1 政府采购项目的采购合同内容的确定应以单一来源采购文件和响应文件为基础，不得违背其实质性内容。本合同将在双方法定代表人或授权代表签字并加盖公章后开始生效。

19.2 本合同一式 6 份，具有同等法律效力。甲方 2 份，乙方 4 份。

19.3 本合同未尽事宜，由双方协商一致另行签订补充协议，补充协议与本合同具有同等法律效力。

（此页仅为签字盖章页）

甲方（公章）：

地址： 通州区留庄路 4 号院 2 号楼

法定代表人或

授权代表（签字）：

日期：2025.11.18

乙方（公章）：

地址：西城区月坛南街 1 号院 2 号楼

法定代表人或

授权代表（签字）：

日期：2025.11.18

乙方（公章）：

地址：东城区东直门外大街 39 号院 2 号

航空服务楼 726 房间

法定代表人或

授权代表（签字）：

日期：2025.11.18

合同附件 1

北京通—养老助残卡管理办法

第一章　总　则

第一条　为规范北京通—养老助残卡的发行、使用和管理，维护持卡老年人的合法权益，提高养老服务科学化、信息化、精准化水平，根据《中华人民共和国老年人权益保障法》和《北京市人民政府办公厅印发<关于加强老年人照顾服务完善养老体系的实施意见>的通知》(京政办发〔2018〕41 号)，制定本办法。

第二条　本办法所称北京通—养老助残卡是由北京市民政局通过政府采购程序确定的银行(以下简称制卡银行)负责制作，为符合条件的老年人免费配发，集社会优待、政策性津贴发放、金融借记账户、市政交通一卡通等多功能于一体的 IC 卡。

第三条　本市行政区域内北京通—养老助残卡的申领、制作、发放、使用及管理等工作，适用本办法。

第四条　办理北京通—养老助残卡的条件为 60 周岁及以上的京籍老年人和持我市有效居住证的常住外埠老年人。

第五条　北京市民政局是北京通—养老助残卡的主管部门，负责制定养老服务相关政策，整合行政和社会资源，协调制卡银行做好卡的制作、发放和结算工作。北京市经济和信息化局负责指导北京通—养老助残卡的技术规范，生成北京通—养老助残卡卡号，负责承担在市政交通一卡通等公共服务领域大规模应用北京通的技术保障和统筹协调职责。北京市交通委员会、文化和旅游局、园林绿化局、公园管理中心负责卡在交通、景区、公园、园林等各部门的使用与管理，保障优待政策的实施。北京市老龄工作委员会办公室负责协调各相关单位落实优待政策。

第六条　北京通—养老助残卡的申领、制发和使用等如发生争议纠纷，由北京市民政局进行协调处理，并委托社会组织开展与卡的业务相关的养老服务工作。

第二章　功能设置

第七条　北京通—养老助残卡是北京市老年人享受社会福利、社会优待及社会服务的身份凭证，具有信息记录、信息查询、业务办理等功能。

第八条　优待功能。老年人持卡享受我市各类社会优待政策，刷卡享受免费乘坐市域内地面公交车(出市域范围按公交管理规定缴费)、免费游览市区级政府投资为主建设并运营管理的公园和景区(国家法定节假日和举办大型活动期间按优待场所相关管理规定执行)，此功能仅限本人使用，满两年后每两年办理一次延期。

第九条　借记功能。北京通—养老助残卡具备银行借记卡功能。借记卡功能激活及使用参照制卡银行相关规定执行。

第十条　政策性功能。北京通—养老助残卡可用于我市各类老年人福利津贴补贴发放，老年人持卡享受居家服务优惠等相关养老服务政策。

第十一条　具有普通市政交通一卡通的基本功能，在指定的充值网点充值后，也可用于非优待范围的其他市政交通一卡通应用领域(如轨道交通等)。

第三章　申请与发放

第十二条　符合办卡条件的老年人首次申请免费。

第十三条　符合办卡条件的老年人在60周岁生日前6个月内到制卡银行网点申请办理北京通—养老助残卡。

第十四条　符合办卡条件的老年人应提供以下材料进行申请：

1.京籍老年人(包括驻京部队离退休军人)提供户口簿及居民身份证原件。

2.外省市老年人提供居民身份证及《居住证》原件。

3.常住外埠离退休军人提供有效身份证件及在京居住6个月以上证明原件。

4.港澳台、归国华侨老年人提供：

(1)护照、港澳居民往来内地通行证、台湾居民来往大陆通行证等有效身份证件原件；

(2)《居住证》或居住6个月以上的《临时住宿登记表》的原件。

5.外国公民提供：

(1)护照原件；

(2)《外国人永久居留证》原件；

(3)《居住证》或居住6个月以上的《临时住宿登记表》的原件。

符合办卡条件的老年人在申请时，如人口数据系统中缺少照片，申请人需自行补充近期一寸标准白底彩色电子照片一张。

第十五条　符合办卡条件的老年人，若委托他人申请办理北京通—养老助残卡，除按上述要求提供有关证件材料外，代办人还需提供本人身份证原件。

第十六条　北京市民政局须对制卡银行采集上报的申请信息进行数据审核，并将审核结果返回制卡银行，由制卡银行告知申请用户审核结果，审核通过的进入制发卡流程。

第十七条　北京通—养老助残卡由制卡银行按照《北京市社会服务一卡通(北京通)卡片技术规范》(DB11/T 1179—2015)标准制卡。

第十八条　制发卡工作在资质审核通过后40个工作日内完成。

第十九条　制卡成功后，老年人或代领人持有效身份证件(代领人还需提供本人身份证原件)到制卡银行领取北京通—养老助残卡，或选择制卡银行寄送服务。

第四章　使用与管理

第二十条　持卡老年人乘坐地面公交车时，上、下车须按规定分别刷卡。若持卡老年人拒绝刷卡乘车，乘务人员有权拒绝其享受乘车优待功能。

免费乘车范围为：除旅游观光线、定制公交等多样化服务专线以外的北京市市域内公交运营线路(出市域范围按公交管理规定缴费)。

持卡老年人乘坐城市轨道交通，费用支付按照相关通用标准执行。参照市政交通一卡通卡，享受北京轨道交通票价政策，包括计程、累计折扣优惠及低峰优惠等。

第二十一条　持卡老年人游览公园、景区时，在装有刷卡设备的公园须刷卡入园，若持卡老年人拒绝刷卡入园，相关工作人员有权拒绝其享受游览优待功能；在没有刷卡设备的公园、景区，按照各公园、景区管理要求入园。

免费游览公园、景区范围为：市、区级政府投资为主并运营管理的公园、景区等(国家法定节假日和举办大型活动期间按优待场所相关管理规定执行)。

第二十二条　北京通—养老助残卡免费乘车、免费游览公园景区的优待功能有效期为两年，有效时间自发行日期起计算，卡片到期后须办理延期方可继续使用。持卡人可在两年有效期前，到制卡银行网点、自助延期终端或通过手机APP等方式办理延期。

第二十三条　北京通—养老助残卡用户办理延期业务需委托子女或他人办理时，除按上述要求提供相关证件材料外，代办人还需提供本人身份证原件。

第二十四条　老年人因户籍变更、死亡等原因不再符合办卡条件时，老年人或其家属须及时向银行申请中止、注销北京通—养老助残卡，按相关政策规定处理账户资金。

第二十五条　北京市民政局须建立老年人信息核查机制，定期对老年人的户籍及生存状况进行数据核查，按规定对核查结果进行处理，对不符合条件的卡片的优待功能进行中止和注销。

第二十六条　北京通—养老助残卡如有丢失，持卡人应及时挂失，具体挂失程序按照制卡银行规定的程序办理。

第二十七条　北京通—养老助残卡丢失或损坏需重新办理时，按本办法第三章要求办理。北京通—养老助残卡因丢失或人为损坏需重新换卡时，工本费由持卡人本人承担，具体费用按制卡银行规定执行。补换卡期间不影响政府政策补贴资金的发放。

第二十八条　老年人在申办或使用北京通—养老助残卡过程中，因制卡失败或技术性损坏等原因未能及时领取或使用卡片，可向制卡银行免费申领临时卡。

第二十九条　临时卡采用实名制办理，使用时须附持卡人照片，制卡时间为 5 个工作日，有效期为 2 个月。具有公交、公园刷卡功能，过期失效。临时卡不能办理挂失、补办业务。

第三十条　待制卡或换卡成功后，本人或代办人领卡时须向制卡银行交回临时卡，拒不交回临时卡者，制卡银行将报北京市民政局进行处理。若用户丢失临时卡，则须按照制卡银行规定缴纳工本费。

第三十一条　持卡人在使用金融、一卡通相关功能时，须执行相关行业规定，遵守安全管理要求。

第五章　责任追究

第三十二条　公民、法人或者其他组织认为北京通—养老助残卡经办机构或相关业务部门在北京通—养老助残卡的发放、使用、管理等过程中有违法行为的，可以向监察部门或北京市民政局举报。

第三十三条　北京通—养老助残卡经办机构或相关业务部门有下列情形的，由民政部门责令整改；给申请人造成经济损失的，由所在单位或者上级主管部门依法追究当事人责任并责令其承担赔偿责任；情节严重的对直接责任人员给予处分；构成犯罪的，依法移送司法机关追究刑事责任。

(一)不依法履行发卡职责的；

(二)违法收取费用的；

(三)违法使用用户个人信息的；

(四)未采取安全措施造成持卡人合法权益受到损害的；

(五)其他违规违法行为。

第三十四条　有下列情形的，由市民政局对卡进行处置，中止卡的相关功能。持卡人违反相关规定的，由相关部门和单位按规定处理。涉嫌犯罪的，依法移送司法机关追究刑事责任。

(一)使用过期、作废的北京通—养老助残卡或临时卡的；

(二)使用他人的北京通—养老助残卡或临时卡的；

(三)提供虚假材料申领北京通—养老助残卡或临时卡的；

(四)伪造、变造北京通—养老助残卡或临时卡的；

(五)使用伪造、变造的北京通—养老助残卡或临时卡的。

第六章　附　则

第三十五条　本办法自2019年1月1日起施行，原《北京通—养老助残卡管理办法(暂行)》(京民老龄发〔2016〕431号)同时废止。

第三十六条　本办法由北京市民政局负责解释。

合同附件 2　乙方服务人员清单

拟担任 职务、分工	姓名	职称	专业	从业资格	相关工作年限
项目牵头人	张莉静	中级会计师	硕士研究生	银行业额从业资格、金融理财师	18 年
技术牵头人	李茜	中级经济师	硕士研究生	银行业额从业资格	22 年
成员	关蕾	中级经济师	硕士研究生	银行业额从业资格、金融理财师	16 年
成员	唐柯		本科	银行从业资格	13 年
成员	连浩		本科	银行从业资格	8 年
（以上为农商银行服务人员，以下为公交公司服务人员）					
项目负责人	寇鸣		本科		19 年
项目运营负责人	于鸿涛		本科		23 年
技术牵头人	邢钊		本科		19 年
实名系统运营维护负责人	陈嘉楠		本科		11 年
数据分析 牵头人	刘世俊	中级	本科		13 年
卡务管理负责人	蒋金煜		本科		15 年
POS 机技术支持	苗桐瑀		本科		8 年
公园项目负责人	徐海鹏		本科		13 年
公交终端项目负责人	王嘉欢		本科		8 年
客服服务主管	李强		本科		8 年

合同附件3《北京市社会服务一卡通（北京通）卡片技术规范》（DB11/T 1179-2015）

ICS 35.240.60
L 67
备案号：45818-2015

DB11

北 京 市 地 方 标 准

DB11/T 1179-2015

社会服务一卡通（北京通）卡片技术规范

Technology specification for social services card (Beijing card)

2015-04-30 发布　　2015-06-01 实施

北京市质量技术监督局 发布

目　次

前　言

本标准按照 GB/T 1.1-2009 给出的规则起草。

本标准由北京市经济和信息化委员会提出并归口。

本标准由北京市经济和信息化委员会组织实施。

本标准起草单位：北京市经济和信息化委员会、北京中电华大电子设计有限责任公司、中国农业银行股份有限公司北京市分行、北京数字认证股份有限公司、北京市政交通一卡通公司、北京德鑫泉物联网科技股份有限公司、大唐微电子技术有限公司、太极计算机股份有限公司、北京华大智宝电子系统有限公司、中国软件与技术服务股份有限公司。

本标准主要起草人：张伯旭、童腾飞、潘锋、沈丽普、高顺尉、韩鹏、李佳、葛晨、傅佳杰、李中元、闫晗、尹寒、张晓冬、焦华清、黄圆圆、陈跃、程智友。

社会服务一卡通（北京通）卡片技术规范

1 范围

本标准规定了社会服务一卡通（以下简称北京通）卡种类、卡介质、机电特性与通讯协议、应用构成、密钥管理、文件和数据规划、应用选择、北京通应用流程和安全机制等方面的内容。

本标准适用于北京通卡的设计、制造、管理、发行和应用。

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，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 2260 中华人民共和国行政区划代码
GB/T 2261.1 个人基本信息分类与代码 第1部分：人的性别代码
GB/T 3304 中国各民族名称的罗马字母拼写法和代码
GB/T 7408 数据元和交换格式 信息交换 日期和时间表示法
GB 11643 公民身份号码
GB/T 14916 识别卡 物理特性
GB/T 16649（所有部分）识别卡 带触点的集成电路卡
GA 214.3 常住人口管理信息规范 第3部分：居民身份证管理信息数据项
GA 461 居民身份证制证用数字相片技术要求
LD/T 32 （所有部分）社会保障卡规范
JR/T 0025（所有部分） 中国金融集成电路（IC）卡规范
DB11/T 159（所有部分） 市政交通一卡通技术规范
ISO/IEC 14443（所有部分） 识别卡 非接触式集成电路卡 接近式卡

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

北京通应用 Beijing tong application
北京通卡中与社保、金融、交通等应用并存，且有独立密钥控制的一个应用。

3.1.2

CPU 卡 central processing unit card
带有中央处理器（CPU）、存储单元以及芯片操作系统的集成电路卡。

3.1.3

芯片 chip

卡中用于完成数据处理和存储功能的集成电路器件。

3.1.4

芯片操作系统 chip operating system（COS）

CPU 卡芯片中存储和可运行的，保护应用数据和程序的机密性和完整性、控制CPU 卡芯片与外界信息交换的嵌入式软件。

3.1.5

命令 command

终端向 IC 卡发出的一条信息，该信息启动一个操作或请求一个应答。

3.1.6

连接 concatenation

两个元素的连接是指将第二个元素附加到第一个元素的末尾。

注：每个元素的字节在结果串中的排列顺序与其从 IC 卡发送到终端的顺序相同，即：高位字节先送。每个字节位按照从最高位到最低位的顺序排列。一组元素或对象可以通过最先两个相连的方式连接成一个新元素，即第一个与第二个相连，再与第三个相连，…，依次类推。

3.1.7

触点 contact

在集成电路卡和外部接口设备之间保持电流连续性的导电元件。

3.1.8

响应 response

IC 卡处理完成收到的命令报文后，返回给终端的报文。

3.1.9

交易 transaction

持卡者和业务、管理部门之间根据卡所支持的应用接受、提供服务的行为。

3.1.10

功能 function

由一个或多个命令实现的处理过程，其操作结果用于完成全部或部分交易。

3.1.11

报文 message

由终端向卡或卡向终端发出的，不含传输控制字符的字节串。

3.1.12

报文鉴别代码 message authentication code

对交易数据及其相关参数进行运算后产生的、用于验证报文完整性的代码。

3.1.13

明文 plain text
没有加密的信息。

3.1.14

密文 cipher text
通过密码系统产生的不可理解的文字或信号。

3.1.15

密钥 key
控制加密转换操作的符号序列。

3.1.16

加密算法 cryptographic algorithm
为了隐藏或揭露信息内容而变换数据的算法。

3.1.17

对称加密技术 symmetric cryptographic technique
发送方和接收方使用相同保密密钥进行数据变换的加密技术。

3.1.18

非对称加密技术 asymmetric cryptographic technique
采用两种相关变换进行加密的技术，一种是公开变换（由公共密钥定义），另一种是私有变换（由私有密钥定义）。这两种变换具有以下属性，即私有变换不能通过给定的公开变换导出。

3.1.19

私有密钥 private key
一个实体的非对称密钥对中仅供实体自身使用的密钥，在数字签名模式中，私有密钥用于签名功能。

3.1.20

公共密钥 public key
一个实体的非对称密钥对中可以公开的密钥，在数字签名模式中，公共密钥用于验证功能。

3.1.21

保密密钥 secret key
对称加密技术中仅供指定实体所用的密钥。

3.1.22

数字签名 digital signature

对数据的一种非对称加密变换。该变换使数据接收方确认数据的来源和完整性，保护数据发送方发出和接收方收到的数据不被第三方篡改，也保护数据发送方发出的数据不被接收方篡改。

3.1.23

数字证书（或证书） digital certificate

由国家认可的，具有权威性、可信性和公正性的第三方证书认证机构（CA）进行数字签名的一个可信的数字化文件。数字证书包括公开密钥拥有者的信息、公开密钥、签名算法和CA的数字签名。

3.1.24

数据完整性 data integrity

数据不受未经许可的方法变更或破坏的属性。

3.1.25

T=0 协议 T=0 protocol

面向字符的异步半双工传输协议。

3.2 缩略语

下列缩略语适用于本文件。

ADF（Application Definition File）应用数据文件

AID（Application Identifier）应用标识符

an（Alphanumeric）字母数字型

APDU（Application Protocol Data Unit）应用协议数据单元

ATQA（Answer To reQuest, Type A）Type A 的请求应答

ATR（Answer To Reset）复位应答

ATS（Answer To Select, Type A）Type A 的选择应答

B（Binary）二进制

CLA（Chip Card Payment Service）命令类别

cn（Compressednumeric）压缩数字

DDF（Directory Definition File）目录数据文件

DF（Dedicated File）专用文件

EF（Elementary File）基本文件

F（Frequency）频率

FCI（File Control Information）文件控制信息

FID（File Identifier）文件标识符

INS（Instruction Byte of Command Message）命令报文的指令字节

Lc（Exatct Length of Data Sent）终端发出的命令数据的实际长度

Le（Maximum Length of Data Expected）响应数据中的最大期望长度

MAC（Message Authentication Code）报文鉴别代码

MF（Mater File）主控文件

N（Numeric）数字型

NFC（Near Field Communication）近场通信

O（Optional）可选型

P1（Parameter 1）参数1
P2（Parameter 2）参数2
PIN（Personal Identification Number）个人密码
PPS（Protocol and Parameters Selection）协议和参数选择
RATS（Request for Answer To Select, Type A） Type A 的选择应答请求
REQA（REQuest command, Type A） Type A 的请求命令
SAM（Secure Access Module） 安全存取模块
SAK（Select AcKnowledge, Type A） Type A 的选择确认
SW1（Status Word One）状态码1
SW2（Status Word Two）状态码2
SM1（SM1 Cryptographic Algorithm）国家密码管理局发布的密码分组标准对称算法
SM2（SM2 Cryptographic Algorithm）国家密码管理局发布的椭圆曲线公钥密码算法
SM3（SM3 Cryptographic Algorithm）国家密码管理局发布的密码杂凑算法
TLV（Tag Length Value）标签、长度、值
WUPA（Wake-UP command, Type A） Type A 的唤醒命令

4 卡种类

4.1 北京通社保卡

4.1.1 北京通社保卡包括北京通应用、社保应用、金融应用、交通应用、健康应用、自主应用等。

4.1.2 发放对象为在京缴纳社保的常住居民（含北京户籍人口和非北京户籍人口）。

4.2 北京通基本卡

4.2.1 北京通基本卡包括北京通应用、金融应用、交通应用、健康应用、自主应用等。

4.2.2 发放对象为在京未缴纳社保的常住居民（含北京户籍人口和非北京户籍人口）。

4.3 北京通临时卡

4.3.1 北京通临时卡包括北京通应用、交通应用、健康应用、自主应用等。

4.3.2 发放对象为临时来京人员。

5 北京通号

5.1 采用映射降位的办法，对 18 位身份证号码进行压缩，降位至 12 位数字。
5.2 无身份证号人员参照身份证号格式进行编码并压缩。

6 卡介质

6.1 芯片要求

a) 双界面、高性能、安全可控的CPU芯片；
b) 应用存储空间不低于80K；
c) 符合GB/T 16649关于芯片的要求；

d) 符合ISO/IEC 14443 TYPE A关于芯片的要求；
e) 符合JR/T 0025关于芯片的要求；
f) 符合DB11/T 159关于芯片的要求；
g) 符合LD/T 32关于芯片的要求；
h) 符合《居民健康卡技术规范》关于芯片的要求。

6.2 COS 要求

a) 符合JR/T 0025关于COS的要求；
b) 符合DB11/T 159关于COS的要求；
c) 符合LD/T 32关于COS的要求；
d) 符合《居民健康卡技术规范》关于COS的要求；
e) 符合《北京社会保障（个人）卡公钥密码应用规范》要求。

6.3 卡体材料

应使用环保材料。

6.4 卡片外形规格

卡片外形尺寸应符合 GB/T 14916 中对卡规格的规定。

表1 标准卡片尺寸

参数	尺寸	公差
卡片宽度 L	85.60mm	85.47 mm -85.72 mm
卡片高度 W	53.98mm	53.92 mm -54.03 mm
卡片厚度 T	0.81mm	±0.03mm
倒角半径 R	3.18mm	±0.30mm

注：倒角是在圆柱型工件的末端加工出一个具有角度的边。

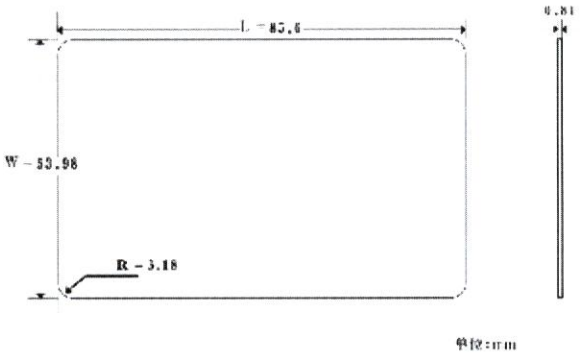


图1 卡片外形

6.5 卡面规范

6.5.1 北京通社保卡面规范

6.5.1.1 卡 A 面要素及布局

卡A面遵循LD/T 32的要求。卡A面应包括以下要素：国徽、卡名（中华人民共和国社会保障卡）。卡A面布局见图2和表2。

图2　北京通社保卡A面布局

表2　北京通社保卡A面布局参数

参数	规格及要求	公差
国徽		
图案	中华人民共和国国徽	
中心到卡的左边沿的距离	42.80mm	±0.25mm
上边沿到卡的下边沿的距离	46.00mm	±0.25 mm
下边沿到卡的下边沿的距离	27.00mm	±0.25 mm
中华人民共和国社会保障卡		
"中华人民共和国"字样	宋体4号	/
左边沿到卡的左边沿的距离	26.00mm	±0.25 mm
下边沿到卡的下边沿的距离	20.00mm	±0.25 mm
"社会保障卡"字样	隶书2号加粗	/
左边沿到卡的左边沿的距离	20.00mm	±0.25 mm
下边沿到卡的下边沿的距离	10.00mm	±0.25 mm

6.5.1.2　卡B面要素及布局

6.5.1.2.1　卡B面应包括以下要素：北京通标识区、金融标识、银行定义区、持卡人照片、持卡人个人信息区、接触式IC芯片、发卡单位信息区、二维码、功能标志区、制卡厂商代码区等。卡片指定区域可以包括地方人力资源社会保障自定义内容（照片有阴框区域）。

6.5.1.2.2　卡B面参考布局及各区域内容说明见图3和表3。

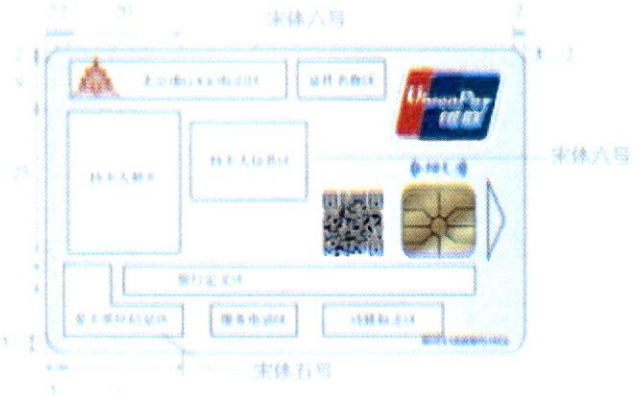


图3 北京通社保卡B面布局

表3 北京通社保卡B面布局参数

参数	规格及要求	公差
北京通标识区		
区域高度	5.00mm	±0.10mm
区域长度	56.00mm	±0.10mm
区域上边距离卡片上边沿	2.00mm	±0.30mm
区域左边距离卡片左边沿	4.00mm	±0.30mm
区域内容	北京通标识、编码	
北京通编码	宋体六号 12位	
证件名称区		
区域高度	5.00mm	±0.10mm
区域长度	15.00mm	±0.10mm
“证件名称”字体	宋体六号	/
“证件名称”左边沿到卡的左边沿的距离	45.00mm	±0.30mm
“证件名称”上边沿到卡的上边沿的距离	2.00mm	±0.30mm
“证件名称”内容	残疾人证、老年人证和学生证等	
金融标识		
金融标识的高度	15.00mm	±0.30mm
金融标识的投影宽度	22.00mm	±0.30mm
金融标识图案与上、下边框间的距离	1.60mm	±0.15mm
金融标识右上端外框边沿垂直线与同侧卡片边沿间的距离	2.00mm	±0.30mm
金融标识上方水平外框边沿与同侧卡片边沿间的距离	2.00mm	±0.30mm
金融标识右上角、左下角的圆角半径	2.00mm	±0.30mm
持卡人照片区		
“照片”的宽度	20.00mm	±0.10mm

表 3（续）

参数	规格及要求	公差
“照片”的高度	25.00mm	±0.10mm
“照片”左边沿到卡的左边沿的距离	4.00mm	±0.30mm
“照片”上边沿到卡的上边沿的距离	11.00mm	±0.30mm
持卡人个人信息区		
持卡人信息内容	姓名、社会保障号码、发证日期	
“姓名”字体	宋体六号	/
“姓名”左边沿到卡的左边沿的距离	28.00mm	±0.30mm
“姓名”上边沿到卡的上边沿的距离	14.50mm	±0.30mm
“社会保障号码”字体	宋体六号	/
“社会保障号码”左边沿到卡的左边沿的距离	28.00mm	±0.30mm
发证日期	宋体六号	/
二维码定义区		
内容大小	不大于 80 字节	
内容信息	使用须知、服务网站、服务电话、监督电话 支持扫描进入服务网站或 APP 下载	
二维码宽度	12.3mm	±0.30mm
二维码高度	12.3mm	±0.30mm
码制	发卡单位自行定义	
接触式 IC 芯片		
触点的最小尺寸和芯片位置	符合 GB/T 16649.2 中相关要求和规定	
插卡方向箭头标识		
标识宽度	2.50mm	±0.10mm
标识高度	10.00mm	±0.10mm
标识右边距离卡片右边	2.00mm	±0.30mm
标识下边距离卡片下边	19.00mm	±0.30mm
发卡单位信息区		
区域长度	20.00mm	±0.10mm
区域高度	10.00mm	±0.10mm
区域右边到卡片的右边	21.00mm	±0.30mm
区域下边到卡片的下边	3.00mm	±0.30mm
区域左边到卡片的左边沿	3.00mm	±0.30mm
发卡单位信息内容	发卡单位名称或印章	
发卡单位名称字体	宋体五号	
印章的直径	12.00mm	±0.10mm
印章上边沿到卡片的上边沿的距离	37.00mm	±0.30mm
印章左边沿到卡的左边沿的距离	2.00mm	±0.30mm
银行定义区		
区域长度	60.00mm	±0.10mm
区域高度	6.00mm	±0.10mm

表 3（续）

参数	规格及要求	公差
区域右边到卡片的右边	5.00mm	±0.30mm
区域下边到卡片的下边	7.00mm	±0.30mm
区域内容	合作银行标识、银行卡号	
区域左边首位的中心距离卡片左边	15.5mm	±0.20mm
区域左边首位的中心距离卡片下边	12.5mm	±0.20mm
服务电话信息		
区域长度	15.00mm	±0.10mm
区域高度	4.00mm	±0.10mm
“服务电话”下边沿到卡片下边沿	2.00mm	±0.30mm
“服务电话”左边沿到卡片左边沿	2.00mm	±0.30mm
制卡厂商代码区		
制卡厂商代码区宽度	15.00mm	±0.10mm
制卡厂商代码区高度	1.50mm	±0.10mm
区域右边距离卡片右边	2.00mm	±0.30mm
区域下边距离卡片下边	2.00mm	±0.30mm
功能标志区		
功能标志区宽度	8.00mm	±0.30mm
功能标志区高度	4.00mm	±0.30mm
功能标志区内容	功能标志	

6.5.1.2.3　卡 B 面部分要素的表示形式见表 4。

表4　北京通社保卡 B 面要素表示形式

参数	表示形式
姓名	使用汉字。当姓名长度超过 6 个汉字时，通过缩小字号或缩小字号并换行处理。
社会保障号码	符合 GB 11643 规定
持卡人照片	符合 GA 461 规定
发卡单位印章	发卡单位印章
二维码	完整

6.5.2　北京通基本卡面规范

6.5.2.1　卡 A 面要素及布局

卡 A 面应包括北京通标识、“北京市社会服务通”等内容，卡 A 面布局见图 4 和表 5。

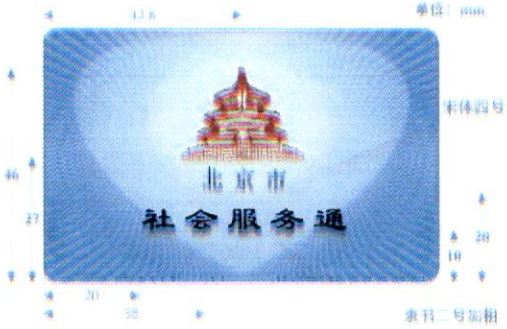


图4　北京通基本卡 A 面布局

表5　北京通基本卡 A 面布局参数

参数	规格及要求	公差
北京通标识		
图案	天坛外形 内嵌北京通字样	/
中心到卡的左边沿的距离	42.80mm	±0.25mm
上边沿到卡的下边沿的距离	46.00mm	±0.25 mm
下边沿到卡的下边沿的距离	27.00mm	±0.25 mm
北京市社会服务通		
"北京市"字样	宋体四号	/
左边沿到卡的左边沿的距离	36.00mm	±0.25 mm
下边沿到卡的下边沿的距离	20.00mm	±0.25 mm
"社会服务通"字样	隶书三号加粗	/
左边沿到卡的左边沿的距离	20.00mm	±0.25 mm
下边沿到卡的下边沿的距离	10.00mm	±0.25 mm

6.5.2.2　卡 B 面要素及布局

6.5.2.2.1　卡 B 面要素包括北京通标识区、证件名称区、金融标识、芯片区、二维码、照片、持卡人个人信息区、发卡单位标识区、服务电话区、银行定义区、功能标志区、制卡厂商代码区等。

6.5.2.2.2　卡 B 面参考布局及各区域内容说明见图 5 和表 6。

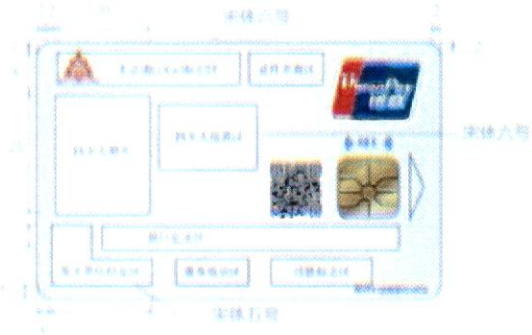


图5　北京通基本卡 B 面布局

表6　北京通基本卡 B 面布局参数

参数	规格及要求	公差
北京通标识区		
区域高度	5.00mm	±0.10mm
区域长度	56.00mm	±0.10mm
区域上边距离卡片上边沿	2.00mm	±0.30mm
区域左边距离卡片左边沿	4.00mm	±0.30mm
区域内容	北京通标识、编码	
北京通编码	宋体六号 12 位	
证件名称区		
区域高度	5.00mm	±0.10mm
区域长度	15.00mm	±0.10mm
“证件名称”字体	宋体六号	/
“证件名称”左边沿到卡的左边沿的距离	45.00mm	±0.30mm
“证件名称”上边沿到卡的上边沿的距离	2.00mm	±0.30mm
“证件名称”内容	残疾人证、老年人证和学生证等	
金融标识		
金融标识的高度	15.00mm	±0.30mm
金融标识的投影宽度	22.00mm	±0.30mm
金融标识图案与上、下边框间的距离	1.60mm	±0.15mm
金融标识右上端外框边沿垂直线与同侧卡片边沿间的距离	2.00mm	±0.30mm
金融标识上方水平外框边沿与同侧卡片边沿间的距离	2.00mm	±0.30mm
金融标识右上角、左下角的圆角半径	2.00mm	±0.30mm
持卡人照片区		
“照片”的宽度	20.00mm	±0.10mm
“照片”的高度	25.00mm	±0.10mm
“照片”左边沿到卡的左边沿的距离	4.00mm	±0.30mm

表 6 （续）

参数	规格及要求	公差
“照片”上边沿到卡的上边沿的距离	11.00mm	±0.30mm
持卡人个人信息区		
持卡人信息内容	姓名、编号、发证日期	
“姓名”字体	宋体六号	/
“姓名”左边沿到卡的左边沿的距离	28.00mm	±0.30mm
“姓名”上边沿到卡的上边沿的距离	14.50mm	±0.30mm
“编号”字体	宋体六号	/
“编号”左边沿到卡的左边沿的距离	28.00mm	±0.30mm
发证日期	宋体六号	/
二维码定义区		
内容大小	不大于 80 字节	
内容信息	使用须知、服务网站、服务电话、监督电话 支持扫描进入服务网站或 APP 下载	
二维码宽度	12.3mm	±0.30mm
二维码高度	12.3mm	±0.30mm
码制	由发卡单位自行定义	
接触式 IC 芯片		
触点的最小尺寸和芯片位置	符合 GB/T 16649.2 中相关要求和规定	
插卡方向箭头标识		
标识宽度	2.50mm	±0.10mm
标识高度	10.00mm	±0.10mm
标识右边距离卡片右边	2.00mm	±0.30mm
标识下边距离卡片下边	19.00mm	±0.30mm
发卡单位信息区		
区域长度	20.00mm	±0.10mm
区域高度	10.00mm	±0.10mm
区域右边到卡片的右边	21.00mm	±0.30mm
区域下边到卡片的下边	3.00mm	±0.30mm
区域左边到卡片的左边沿	3.00mm	±0.30mm
发卡单位信息内容	发卡单位名称或印章	
发卡单位名称字体	宋体五号	
印章的直径	12.00mm	±0.10mm
印章上边沿到卡片的上边沿的距离	37.00mm	±0.30mm
印章左边沿到卡的左边沿的距离	2.00mm	±0.30mm
银行定义区		
区域长度	60.00mm	±0.10mm
区域高度	6.00mm	±0.10mm
区域右边到卡片的右边	5.00mm	±0.30mm
区域下边到卡片的下边	7.00mm	±0.30mm

表 6 （续）

参数	规格及要求	
区域内容	合作银行标识、银行卡号	
区域左边首位的中心距离卡片左边	15.5mm	±0.20mm
区域左边首位的中心距离卡片下边	12.5mm	±0.20mm
服务电话信息		
区域长度	15.00mm	±0.10mm
区域高度	4.00mm	±0.10mm
“服务电话”下边沿到卡片下边沿	2.00mm	±0.30mm
“服务电话”左边沿到卡片左边沿	2.00mm	±0.30mm
制卡厂商代码区		
制卡厂商代码区宽度	15.00mm	±0.10mm
制卡厂商代码区高度	1.50mm	±0.10mm
区域右边距离卡片右边	2.00mm	±0.30mm
区域下边距离卡片下边	2.00mm	±0.30mm
功能标志区		
功能标志区宽度	8.00mm	±0.30mm
功能标志区高度	4.00mm	±0.30mm
功能标志区内容	功能标志	

6.5.2.2.3　卡 B 面要素的表示形式见表 7。

表7 北京通基本卡 B 面要素表示形式

参数	表示形式
姓名	使用汉字。当姓名长度超过 6 个汉字时，通过缩小字号或缩小字号并换行处理。
编号	符合 GB 11643 规定
持卡人照片	符合 GA 461 规定
二维码	完整

6.5.3　北京通临时卡卡面规范

6.5.3.1　卡 A 面要素及布局

卡 A 面应包括以下要素：北京通标识、“北京市社会服务通”。卡 A 面布局见图 6 和表 8。

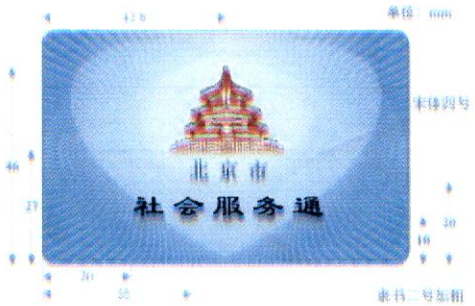


图6 卡A面布局

表8 卡A面布局参数

参数	规格及要求	公差
北京通标识		
图案	天坛外形 内嵌"北京通"字样	/
中心到卡的左边沿的距离	42.80mm	±0.25mm
上边沿到卡的下边沿的距离	46.00mm	±0.25 mm
下边沿到卡的下边沿的距离	27.00mm	±0.25 mm
北京市社会服务通		
"北京市"字样	宋体四号	/
左边沿到卡的左边沿的距离	36.00mm	±0.25 mm
下边沿到卡的下边沿的距离	20.00mm	±0.25 mm
"社会服务通"字样	隶书二号加粗	/
左边沿到卡的左边沿的距离	20.00mm	±0.25 mm
下边沿到卡的下边沿的距离	10.00mm	±0.25 mm

6.5.3.2 卡B面要素及布局

6.5.3.2.1 卡B面要素包括北京通标识区、芯片、二维码、持卡人信息区、发卡单位信息区、服务电话区等。

6.5.3.2.2 卡B面参考布局见图7和表9。

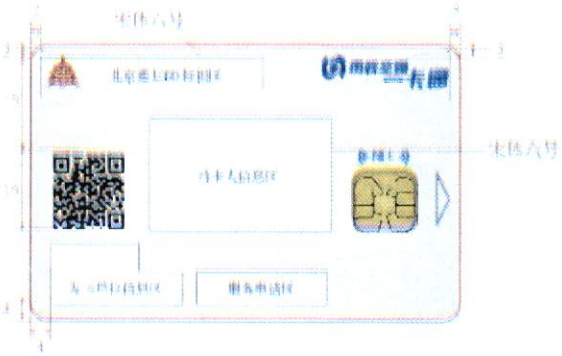


图7 卡B面布局

表9 卡B面布局参数

参数	规格及要求	公差
北京通标识区		
区域高度	5.00mm	±0.10mm
区域长度	56.00mm	±0.10mm
区域上边距离卡片上边沿	2.00mm	±0.30mm
区域左边距离卡片左边沿	4.00mm	±0.30mm
区域内容	北京通标识、编码	
北京通编码	宋体六号 12位	
持卡人个人信息区		
持卡人信息内容	姓名、编号、发证日期	
“姓名”字体	宋体六号	/
“姓名”左边沿到卡的左边沿的距离	28.00mm	±0.30mm
“姓名”上边沿到卡的上边沿的距离	14.50mm	±0.30mm
“编号”字体	宋体六号	/
“编号”左边沿到卡的左边沿的距离	28.00mm	±0.30mm
发证日期	宋体六号	/
接触式IC芯片		
触点的最小尺寸和芯片位置	符合GB/T 16649.2中相关要求和规定	
二维码定义区		
内容大小	不大于80字节	
内容信息	使用须知、服务网站、服务电话、监督电话 支持扫描进入服务网站或APP下载	
二维码宽度	12.3mm	±0.30mm
二维码高度	12.3mm	±0.30mm
码制	由发卡单位自行定义	

表 9 （续）

参数	规格及要求	公差
发卡单位信息区		
区域长度	20.00mm	±0.10mm
区域高度	10.00mm	±0.10mm
区域右边到卡片的右边	21.00mm	±0.30mm
区域下边到卡片的下边	3.00mm	±0.30mm
区域左边到卡片的左边沿	3.00mm	±0.30mm
发卡单位信息内容	发卡单位名称或印章	
印章的直径	12.00mm	±0.10mm
印章上边沿到卡片的上边沿的距离	37.00mm	±0.30mm
印章左边沿到卡的左边沿的距离	2.00mm	±0.30mm
服务电话区		
区域长度	15.00mm	±0.10mm
区域高度	4.00mm	±0.10mm
“服务电话”下边沿到卡片下边沿	2.00mm	±0.30mm
“服务电话”左边沿到卡片左边沿	2.00mm	±0.30mm

6.5.3.2.3　卡 B 面要素的表示形式见表 10。

表10　北京通临时卡 B 面要素表示形式

参数	表示形式
姓名	使用汉字。当姓名长度超过 6 个汉字时，通过缩小字号或缩小字号并换行处理。
编号	符合 GB 11643 规定
持卡人照片	符合 GA 461 规定
二维码	完整

7　机电特性与通讯协议

7.1　机电特性

北京通卡的机电特性（包括 IC 卡的物理特性和电气特性）应符合 GB/T 16649 系列标准、ISO/IEC 14443 系列标准的相关要求。

7.2　通讯协议和复位应答

7.2.1　接触接口

7.2.1.1　通讯协议

符合 **T=0** 通讯协议。

7.2.1.2　复位应答（ATR）

7.2.1.2.1　在终端发出复位信号后，IC 卡以一串字节作为应答。这些传输到终端的字节规定了卡和终端之间即将建立的通信的特征。

7.2.1.2.2　北京通卡应支持 PPS 协商高速通讯。

7.2.1.2.3　北京通卡加载北京市社会保障卡应用时，卡片的复位应答（ATR）信息如下：

3B	7x（'0'~'F'）	FiDi	00	00	历史字节（0~15 字节）

其中 FiDi 符合北京市社会保障卡技术要求设定。

其中历史字节定义：

2 字节	3 字节	2 字节	6 字节
芯片商注册标识号	COS 名称和版本	卡制造商注册标识号	唯一序列号

7.2.2 非接触接口

7.2.2.1 通讯协议

7.2.2.1.1 符合 ISO/IEC 14443 TYPE A 通讯协议。

7.2.2.1.2 NFC 通讯协议兼容 ISO/IEC 14443 TYPE A 通讯协议。

7.2.2.1.3 使用 NFC 手机终端与卡片进行数据交换，可以读取卡片信息。

7.2.2.2 复位应答（ATS）

7.2.2.2.1 IC 卡上电检测到处于非接触通讯方式后，等待接收 REQA 或 WUPA 命令，如果接收到 REQA 或 WUPA 命令，则 IC 卡返回 ATQA。

7.2.2.2.2 接收到 ATQA 后，读卡器发出防冲突和选卡指令，当 IC 卡被选中时，IC 卡返回 SAK；读卡器接收到 SAK 后，如果 IC 卡支持 ISO/IEC 14443，则读卡器发送 RATS 命令给 IC 卡，IC 卡接收到 RATS 命令后，返回一个 ATS。

7.2.2.2.3 北京通卡加载居民健康卡应用时，卡片的复位应答（ATS）信息如下：

XX（'05'~'14'）	'78'	TA1	TB1	'02'	历史字节（0~15 字节）

其中，历史字节定义：

2 字节	2 字节	4 字节
芯片商注册标识号	卡片制造商注册标识	唯一序列号

7.2.2.2.4 如卡片加载北京市政交通一卡通应用，则 ATQA 值应符合 DB11/T 159 的规定。

8 应用构成

8.1 北京通社保卡

8.1.1 北京通社保卡应用

北京通社保卡应用包括北京通应用、社保应用、金融应用、交通应用、健康应用、自主应用六个应用。

8.1.2 基本信息

基本信息包含个人信息、照片数据等内容。

8.1.3 证书应用

证书应用可由市民可自主选择加载。

8.1.4 北京通社保卡空间分配

8.1.5

表11　北京通社保卡空间分配表

应用区	通讯方式	应用数据空间	规划内容
基本信息	接触/非接触	3.5K	基本信息 1（218 字节）
			基本信息 2（217 字节）
			照片数据（3K 字节）
北京通应用	接触/非接触	3K	遵循本标准 10.7 的要求
社保应用	接触	16K	遵循 LD/T 32 要求
金融应用	接触/非接触	8K~16K	遵循 JR/T 025 要求
交通应用	非接触	8K	遵循 DB11/T 159 要求
健康应用	非接触	32K	遵循《居民健康卡技术规范》要求
自主应用	接触/非接触	3K	遵循本标准 10.8 的要求，满足社区、街道等应用
证书	接触/非接触	5K	遵循本标准 13.3 的要求

8.2　北京通基本卡

8.2.1　北京通基本卡应用

北京通基本卡包括北京通应用、金融应用、交通应用、健康应用、自主应用五个应用。

8.2.2　基本信息

基本信息包含个人信息、照片数据等内容。

8.2.3　证书应用

证书应用可由市民自主选择加载。

8.2.4　北京通基本卡空间分配

表12　北京通基本卡空间分配表

应用区	通讯方式	应用数据空间	规划内容
基本信息	接触/非接触	3.5K	基本信息 1（218 字节）
			基本信息 2（217 字节）
			照片数据（3K 字节）
北京通应用	接触/非接触	3K	遵循本标准 10.7 的要求
金融应用	接触/非接触	8K~16K	遵循 JR/T 025 要求
交通应用	非接触	8K	遵循 DB11/T 159 要求
健康应用	非接触	32K	遵循《居民健康卡技术规范》要求
自主应用	接触/非接触	3K	遵循本标准 10.8 的要求
证书	接触/非接触	5K	遵循本标准 13.3 的要求

8.3　北京通临时卡

8.3.1　北京通临时卡应用

北京通临时卡包括北京通应用、交通应用、健康应用、自主应用四个应用。。

8.3.2　基本信息

基本信息包含个人信息、照片数据等内容。

8.3.3 证书应用

证书应用可由市民自主选择加载。

8.3.4 北京通临时卡空间分配

表13 北京通临时卡空间分配表

应用区	通讯方式	应用数据空间	规划内容
基本信息	接触/非接触	3.5K	基本信息 1（218 字节）
			基本信息 2（217 字节）
			照片数据（3K 字节）
北京通应用	接触/非接触	3K	遵循本标准 10.7 的要求
交通应用	非接触	8K	遵循 DB11/T 159 要求
健康应用	非接触	32K	遵循《居民健康卡技术规范》要求
自主应用	接触/非接触	3K	遵循本标准 10.8 的要求
证书	接触/非接触	5K	遵循本标准 13.3 的要求

9 密钥管理

9.1 主管理密钥

9.1.1 主管理密钥由主发卡机构管理并生成。

9.1.2 主管理密钥负责创建应用区。

9.2 密钥管理应用构成

表14 密钥管理应用构成

应用区	密钥管理系统
基本信息区	北京通密钥管理系统
北京通应用	北京通密钥管理系统
社保应用	北京社保卡密钥管理系统
金融应用	银行卡密钥管理系统
交通应用	北京一卡通密钥管理系统
健康应用	健康卡密钥管理系统
自主应用	可设置密钥控制

9.3 北京通应用密钥管理

9.3.1 密钥生成

9.3.1.1 密钥的生成方式

密钥采用集中方式生成，由北京通密钥管理系统负责生成相应的主密钥组，其他密钥由该组主密钥分散生成。密钥生成的方式为可重复的密钥生成方式，即采用密钥变换、衍生的生成方式，在需要的情况下，能够重新得到与原来相同的密钥值。

9.3.1.2 密钥生成的安全技术

可重复生成的密钥采用密钥变换或密钥衍生的办法生成，确保密钥变换或密钥衍生的过程安全。

9.3.2 密钥的发行

密钥的发行采用梯级生成、下发。由上一级生成下一级所需的各种子密钥，并以指定形式传递给下一级。

9.3.3 密钥的管理

9.3.3.1 所有涉及到读取或修改卡中敏感数据的交易，应使用加密密钥保证应用的安全性。应用密钥的管理由发卡方负责，见图 15。

表15 用于卡片合法性验证及基本信息管理的应用密钥

分类	密钥	用途	适用的应用范围
鉴别密钥	IRK	鉴别发卡方的密钥	基本信息应用
应用数据更新密钥	UK	发卡方或应用提供方控制应用数据更新操作的密钥	基本信息文件 1、基本信息文件 2、照片信息文件
应用数据读取密钥	RK	发卡方或应用提供方控制部分应用数据读取操作的密钥	基本信息文件 2

9.3.3.2 北京通应用密钥分散流程见附录 C。

9.4 密钥管理系统

各应用密钥管理，遵循各应用管理机构的密钥管理系统要求。

10 文件和数据规划

10.1 基本信息

10.1.1 基本信息文件结构说明

表16 基本信息文件结构说明

应用区	文件标识	文件内容	文件结构	读控制	写控制
基本信息	‘EF05’	基本信息文件 1	变长	无	UK
	‘EF06’	基本信息文件 2	变长	RK	UK
	‘EF07’	照片信息文件	透明	无	UK

10.1.2 数据结构与信息

基本信息区：

a) EF05 基本信息文件 1，见表 17：

表17 EF05 基本信息文件 1

文件标识符	‘EF05’	SFI	‘05’	读控制	无	写控制	UK	文件结构	变长记录
标志	数据项							类型	长度
‘01’	姓名							an	‘1E’

表 17 （续）

文件标识符	'EF05'	SFI	'05'	读控制	无	写控制	UK	文件结构	变长记录
'02'	性别							an	'01'
'03'	北京通号							an	'0C'
'04'	北京通卡的类别							cn	'01'
'05'	证件名称							an	'20'
'06'	发卡机构							an	'20'
'07'	免责声明							an	'3F'
'08'	服务电话以及网站							an	'2F'

1) 姓名：持卡人的姓名应使用全国通用文字，本规范规定卡内存储的姓名用汉字表达；
2) 性别：性别分为未知的性别、男性、女性和未说明的性别等四类。持卡人性别用一个字符的阿拉伯数字代码表示，其表示方法应符合 GB/T 2261.1 的规定；
3) 北京通号：依照本规范第 5 章节规定；
4) 北京通卡的类别:包括北京通社保卡'01'、北京通基本卡'02'、北京通临时卡'03'；
5) 证件名称：证件名称是指此类卡片具有的证件类型，包含残疾人证、学生证、老年人证等内容。可存储多个证件类型，卡内存储的第一个证件类型与卡面证件信息区的内容一致；
6) 发卡机构：发卡机构是指卡片的主发行机构名称；
7) 免责声明：免责声明与卡面上的二维码中的免责声明内容一致；
8) 服务电话及网站：服务电话及网站与卡面上的二维码服务电话及网站内容一致。

b) EF06 基本信息文件 2，见表 18：

表18 EF06 基本信息文件 2

文件标识符	'EF06'	SFI	'06'	读控制	RK	写控制	UK	文件结构	变长记录
标志	数据项							类型	长度
'0A'	民族							cn	'01'
'0B'	出生日期							cn	'04'
'0C'	公民身份证号码							an	'12'
'0D'	固定电话							an	'0F'
'0E'	移动电话							an	'0F'
'0F'	居住地							an	'50'
'10'	户籍地址							an	'50'
'11'	制卡时间							cn	'04'

1) 民族：采用国家认定的民族名称来记录持卡人的民族信息。本规范规定民族名称用二个字符的阿拉伯数字代码表示，其表示方法应符合 GB/T 3304 的规定；
2) 出生日期：出生日期采用公历日期，其表示方法应符合 GB/T 7408 的规定；
3) 公民身份号码：公民身份号码是由公安机关对具有中华人民共和国国籍的公民给出的一个唯一的、终身不变的法定号码。公民身份号码的结构和表示形式应符合 GB 11643 的规定；

4) 固定电话：能与持卡人保持联系的电话号码；
5) 移动电话：能与持卡人保持联系的电话号码；
6) 居住地：持卡人现居住地址。居住地址可以是常住户口地址，也可以是常住户口以外的地址，表示方法应符合 GB /T 2260 的规定；
7) 户籍地址：常住户口所在地地址是指户口所在地的详细地址。常住户口所在地由中华人民共和国行政区划名称、街道（乡、镇）和街、路、巷、村等名称以及门牌号码及居室号码构成。行政区划名称应符合 GB/T 2260 的规定；
8) 制卡时间：卡生成的年和月，按照年/月的格式。

c) EF07 照片信息文件，见表 19：

表19　EF07 照片信息文件

文件标识符	'EF07'	SFI	'07'	读控制	无	写控制	UK	文件结构	透明
标志	数据项							类型	长度
--	照片数据							B	'C00'

其中，照片数据的存储持卡人照片信息，符合 GA 214.3 规定。

注：本章中所定义的所有应用数据的标志、长度都以十六进制值表示。

10.2 社保应用

社保应用文件结构与数据信息，应符合《北京市社会保障卡结构说明》定义。

10.3 金融应用

金融应用文件结构与数据信息，应符合 JR/T 0025 规范定义。

10.4 健康应用

健康应用文件结构与数据信息，应符合《居民健康卡技术规范》定义。

10.5 交通应用

交通应用文件结构与数据信息，应符合 DB11/T 159 规范定义。

10.6 证书应用

证书应用文件结构与数据信息，预留 5K 空间备用。

10.7 北京通应用

北京通应用文件结构与数据信息，预留 3K 空间备用。

10.8 自主应用

预留 3K 空间备用。

11 应用选择

11.1 应用标识符

北京通应用标识符（AID）定义为：D15600001600。AID 的结构应符合 GB/T 16649.5 的规定，包含两个部分：

a) 一个经过注册的应用提供者标识符（长度为 5 字节），它唯一标识应用提供者；

b) 一个可选的专用应用标识符扩展码（PIX）域，最长 11 字节，由应用提供者定义。

11.2 终端的应用选择

表20 终端应用选择方式

应用	通讯方式	应用选择方式	AID	FID	备注
北京通应用	接触/非接触	AID	‘D15600001600’	‘1102’	
社保应用	接触	AID	‘7378312E73682EC9E7BBE1B1A3D5CF’		“Sxl.sh.社会保障”
金融应用	接触/非接触	AID	‘315041592E5359532E4444463031’ ‘325041592E5359532E4444463031’		“1PAY.SYS.DDF01” “2PAY.SYS.DDF01”
居民健康应用	非接触	AID	‘57532E5359532E4444463031’		“WS.SYS.DDF01”
交通应用	非接触	FID		3F00	
基本信息	接触/非接触	AID	‘D15600001601’	1101	
自主应用	接触/非接触	AID	‘D15600001609’	1103	
证书应用	接触/非接触	AID	‘D15600001605’	1104	

注：自主应用应用选择方式可由应用提供方自行定义，AID 为 ASCII 码。

12 北京通应用流程

12.1 北京通应用预处理流程

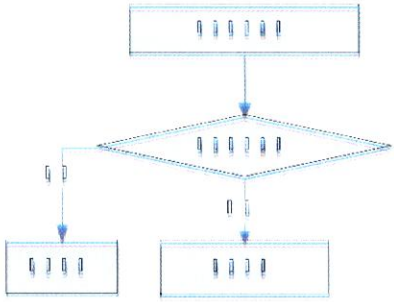


图8 应用预处理流程图

12.1.1 建立通信通道

终端按照GB/T 16649或者ISO/IEC 14443 TYPE A的通信协议方式与进入场内的"北京通卡建立通信通道。

12.1.2 卡有效性检查及持卡人身份认证

检查及认证过程如下：

——首先使用SELECT命令通过AID选择基本信息区；

——然后使用IRK对发卡方进行验证，步骤如下：

a) 终端产生1个8字节的随机数，作为"INTERNAL AUTHENTICATION"命令的数据域；

注：随机数用于产生鉴别数据。

b) 终端发送"INTERNAL AUTHENTICATION"命令，卡将计算鉴别数据并回送；

c) 终端在收到鉴别数据后，进行比较验证。

——如果验证不通过，则退出预处理流程；如果验证通过，则用"READ RECORD"命令读取基本信息数据，终端将对这些数据进行以下检查：

d) 该卡是否在终端存储的黑名单卡之列（使用北京通号）；

e) 终端是否支持从IC卡回送的北京通卡的类别所代表的卡类型；

f) 卡是否在有效期内。

——如果以上任一条件不满足，将进行错误处理；否则，终端继续执行后续步骤。

12.1.3 错误处理

终端对交易预处理出错的处理方法不属于本标准的范围。

12.1.4 应用选择

使用 SELECT 命令通过 AID 对北京通应用进行选择。

12.2 北京通应用处理流程

12.2.1 查询应用信息

12.2.1.1 持卡人或业务管理部门的操作员通过查询应用信息获得卡中想了解的或与办理具体事务相关的信息。

12.2.1.2 该交易对终端是否联机无要求，对应用信息的读取操作仅受终端中 SAM 卡的控制。

12.2.2 更新应用信息

12.2.2.1 业务管理部门的操作员通过更新应用信息在卡中记录持卡人办理具体事务时产生变动的相关信息。

12.2.2.2 该交易对终端是否联机无要求，对应用信息的更新操作仅受终端中 SAM 卡的控制。

12.2.2.3 北京通应用相关指令见附录 A。

13 安全机制

13.1 基本安全要求

13.1.1 共存应用：为了独立地管理一张卡上不同应用间的安全问题，每一个应用单独存放。即在应用之间设计一道“防火墙”，防止跨应用进行非法访问。每一个应用不应与个人化要求和卡中共存的其他应用规则发生冲突；

13.1.2 密钥的独立性：用于一种特定功能（如：读取数据）的加密/解密密钥不能被任何其他功能所使用，包括保存在 IC 卡中的密钥和用来产生、派生、传输这些密钥的密钥；

13.1.3 如果应用要求使用SAM，其对终端、发卡方和私有SAM的安全要求参阅各行业SAM模块规范。

13.1.4 密钥和个人密码存放：在没有授权的情况下，选定的加密/解密算法的非对称私有密钥或对称加密密钥和个人密码都不应被泄露出来。

13.1.5 北京通应用采用的安全计算方法见附录 B。

13.2 加密算法保护

13.2.1 北京通应用、基本信息区应用等使用 SM1 算法进行保护。

13.2.2 社保应用算法遵循《北京社会保障卡结构说明》、《北京社会保障（个人）卡公钥密码应用规范》要求。

13.2.3 金融应用算法遵循 JR/T 0025 要求。

13.2.4 健康应用算法参照《居民健康卡技术标准》要求。

13.2.5 交通应用算法遵循 DB11/T 159 要求。

13.2.6 证书应用使用 SM2、SM3 算法保护。

13.3 报文传输方式

13.3.1 明文模式

如果对数据传输的安全性、完整性以及对发送方的认证都没有要求，可采用明文模式。

13.3.2 加密模式

如果侧重于数据在传输中的安全性，可以采用加密模式。

13.3.3 校验模式

如果侧重于数据在传输中的完整性和对数据发送方进行认证，可采用校验模式。

13.3.4 加密校验模式

如果既要求数据在传输中的安全性又要求数据在传输中的完整性和对数据发送方进行认证，可以采用加密校验模式。

13.4 数字证书

13.4.1 数字证书包括加密证书和签名证书两张证书，用于为持卡人提供身份验证功能和数字签名功能，该两张证书应安全存储在 IC 卡证书应用区内。

13.4.2 数字证书采用 SM2、SM3 等算法，并由具有资质的第三方 CA 认证机构进行签发并提供数字证书生命周期的管理。

附录A
（规范性附录）
北京通应用命令集

A.1 命令报文

A.1.1 命令 APDU 格式

表A.1 命令 APDU 格式

CLA	INS	P1	P2	Lc	Data	Le
←必备头→				←条件体→		

命令 APDU 中发送的数据字节数用 Lc 表示。

响应 APDU 中期望返回的数据字节数用 Le 表示。当 Le 存在且值为 0 时，表示需要最大字节数(256 字节)。

命令 APDU 报文的内容见：

表A.2 命令 APDU 的内容

代码	描　述	长度
CLA	命令类别	1
INS	指令代码	1
P1	指令参数 1	1
P2	指令参数 2	1
Lc	命令数据域中存在的字节数	0 或 1
Data	命令发送的数据字节串(=Lc)	可变
Le	响应数据域中期望的最大数据字节数	0 或 1

A.1.2 响应 APDU 格式

响应 APDU 格式由一个变长的条件体和后随两字节长的必备尾组成：

表A.3 响应 APDU 格式

Data	SW1	SW2
←条件体→	←尾→	

表A.4 响应 APDU 的结构

代码	描　述	长度
Data	响应中接收的数据字节串(=Lr)	变长
SW1	命令处理状态	1
SW2	命令处理限定	1

表A.5　APDU 命令汇总表

序号	命 令	CLA	INS
1	APPEND RECORD	00	E2
2	CARD BLOCK	84	16
3	EXTERNAL AUTHENTICATION	00	82
4	GET CHALLENGE	00	84
5	GET RESPONSE	00	C0
6	INTERNAL AUTHENTICATION	00	88
7	READ BINARY	00	B0
8	READ RECORD	00	B2
9	SELECT FILE	00	A4
10	UPDATE BINARY	00	D6
11	UPDATE RECORD	00	DC
12	COMPUTE SIGNATURE	80	36
13	VERIFY SIGNATURE	80	38
14	PKI ENCIPHER	80	30
15	PKI DECIPHER	80	32
16	GENERATE ENVELOP	80	3A
17	OPEN ENVELOP	80	3C
18	CIPHER DATA	80	3E
19	HASH OPERATION	80	34
20	SM2 KEY EXCHANGE	80	4C
21	SM2 GETZA	80	4E
22	GENERATE KEY PAIR	80	46
23	GET PUBLIC KEY	80	48
24	STORE PKI KEY	80	4A

A.2 北京通应用命令

A.2.1　APPEND RECORD 命令

A.2.1.1　定义和范围

APPEND RECORD 命令用于向记录文件中追加新的记录。对于循环记录文件，可以无限循环追加记录；对于线性记录文件，追加的记录只能追加到文件尾。

A.2.1.2　命令报文

表A.6　命令代码及数值

代码	数值								
CLA	'00'								
INS	'E2'								
P1	'00'								
P2	b8	b7	b6	b5	b4	b3	b2	b1	说　明
	0	0	0	0	0	0	0	0	当前的 EF 文件
	X	x	x	x	X	0	0	0	用 SFI 方式
Lc	后续数据域的长度								
DATA	向记录文件中追加的新记录								
Le	不存在								

A.2.1.3　命令报文数据域

命令报文数据域为向记录文件中追加的新记录。

A.2.1.4　响应报文数据域

响应报文数据域不存在。

A.2.1.5　响应报文状态码

表A.7　响应信息中可能的状态码

SW1	SW2	说　明
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	81	当前文件不是记录文件
69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效
69	85	使用条件不满足
69	86	没有选择当前文件
69	88	安全信息数据错误
6A	81	功能不支持
6A	82	未找到文件
6A	84	记录空间已满
6A	85	Lc 与 TLV 结构不匹配
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

A.2.2　CARD BLOCK 命令

A. 2. 2. 1 定义和范围

CARD BLOCK命令使北京通应用区永久失效。

当CARD BLOCK命令成功地完成后，在北京通应用区内所有后续的命令都将回送状态字“不支持此功能”(SW1 SW2='6A81')，且不执行任何其他操作。

A.2.2.2 命令报文

表A.8 命令代码

代码	数 值
CLA	'84'
INS	'16'
P1	'00'
P2	'00'
Lc	'04'
DATA	报文鉴别码（MAC）
Le	不存在

A.2.2.3 命令报文数据域

命令报文数据域包括报文鉴别码(MAC) 数据元。

A.2.2.4 响应报文数据域

响应报文数据域不存在。

A.2.2.5 响应报文状态字

表A.9 响应信息中可能的状态码

SW1	SW2	含 义
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	83	认证密钥锁定
69	85	使用条件不满足
69	88	安全报文数据项不正确
6A	86	P1,P2 参数错
6D	00	命令不存在
6E	00	CLA 错

A.2.3 EXTERNAL AUTHENTICATE 命令

A.2.3.1 定义和范围

EXTERNAL AUTHENTICATE 命令要求 IC 卡中的应用验证接口设备的有效性，以使接口设备获得某种授权。

A.2.3.2 命令报文

表A.10 命令代码

代码	数值
CLA	'00'
INS	'82'

表 A.10 （续）

代码	数值								
P1	'00'								
P2	b8	b7	b6	b5	b4	b3	b2	b1	说　明
	0	-	-	-	-	-	-	-	全局参考参数
	1	-	-	-	-	-	-	-	局部参考参数
	-	x	x	x	x	x	x	x	密钥标识
	0	0	0	0	0	0	0	0	当前 DF 下的 MK
Lc	'08'								
DATA	鉴别数据（8 字节）								
Le	不存在								

A.2.3.3　命令报文数据域

8字节鉴别数据。

A.2.3.4　响应报文数据域

响应报文数据域不存在。

A.2.3.5　响应报文状态码

表A.11　响应信息中可能的状态码

SW1	SW2	说明
90	00	命令执行成功
63	Cx	认证失败，还可认证 x 次
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效
69	85	使用条件不满足
6A	81	功能不支持
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

A.2.4　GET CHALLENGE 命令

A.2.4.1　定义和范围

GET CHALLENGE 命令从卡中读取与安全相关的随机数，用于接着的安全相关过程。

A.2.4.2　命令报文

表A.12　命令代码

代码	数值
CLA	'00'
INS	'84'
P1	'00'
P2	'00'
Lc	不存在
DATA	不存在
Le	'04'或'08' 或'10'

A.2.4.3　命令报文数据域

命令报文数据域不存在。

A.2.4.4　响应报文数据域

响应报文数据域包括随机数，长度为4字节或8字节或16字节。

A.2.4.5　响应报文状态码

表A.13　响应信息中可能的状态码

SW1	SW2	说明
90	00	命令执行成功
67	00	Lc 长度错误
6A	81	功能不支持
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错

A.2.5　GET RESPONSE 命令

A.2.5.1　定义和范围

当 APDU 不能用现有协议传输时，GET RESPONSE 命令提供了一种从卡片向接口设备传送 APDU(或 APDU 的一部分)的传输方法。

A.2.5.2　命令报文

表A.14　命令代码

代码	数值
CLA	'00'
INS	'C0'
P1	'00'
P2	'00'
Lc	不存在
DATA	不存在
Le	响应的最大数据长度

A.2.5.3 命令报文数据域

命令报文数据域不存在。

A.2.5.4 响应报文数据域

响应报文数据域的长度由 Le 的值决定。

如果 Le 的值为零，在附加数据有效时，卡片应回送状态码'6CXX'，否则回送状态码'6F00'。

A.2.5.5 响应报文状态码

响应报文数据域的长度由 Le 的值决定。

如果 Le 的值为零，在附加数据有效时，卡片应回送状态码'6CXX'，否则回送状态码'6F00'。

表A.15 响应信息中可能的状态码

SW1	SW2	说明
90	00	命令执行成功
61	xx	还有 xx 字节需要返回
67	00	Le 长度错误
6A	86	P1、P2 参数错
6C	xx	长度错误，'xx'表示实际长度
6D	00	命令不存在
6E	00	CLA 错
6F	00	数据无效

A.2.6 INTERNAL AUTHENTICATE 命令

A.2.6.1 定义和范围

INTERNAL AUTHENTICATION 命令提供了利用接口设备发来的随机数和自身存储的相关密钥进行数据认证的功能。

A.2.6.2 命令报文

表A.16 命令代码

代码	数值
CLA	'00'
INS	'88'
P1	'00'
P2	'00'
Le	'08'
DATA	鉴别数据输入因子（8 字节）
Le	'08'鉴别数据

A.2.6.3 命令报文数据域

命令报文数据域为8字节鉴别数据输入因子。

A.2.6.4 响应报文数据域

响应报文数据域内容是相关鉴别数据。

A.2.6.5 响应报文状态码

表A.17 响应信息中的数据

说 明	长 度（字节）
鉴别数据	8

表A.18 响应信息中可能的状态码

SW1	SW2	说 明
90	00	命令执行成功
67	00	Lc 长度错误
69	82	不满足安全状态
69	85	使用条件不满足
6A	81	功能不支持
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

A.2.7 READ BINARY 命令

A.2.7.1 定义和范围

READ BINARY 命令用于读出透明文件的内容。

A.2.7.2 命令报文

表A.19 命令代码

代码	数值								
CLA	'00'								
INS	'B0'								
P1	b8	b7	b6	b5	b4	b3	b2	b1	说明
	0	x	x	x	x	x	x	x	当前 EF 文件偏移地址高字节
	1	0	0	x	x	x	x	x	通过 SFI 方式访问
P2	若 P1 的 b8=0，偏移地址低字节 若 P1 的 b8=1，偏移地址								
Lc	不存在								
DATA	不存在								
Le	期望返回的明文字节数								

A.2.7.3 命令报文数据域

命令报文数据域不存在。

A.2.7.4 响应报文数据域

当Le的值为零时，只要文件的最大长度在256(短长度)或65536(扩展长度)之内，则其全部字节将被读出。

A.2.7.5 响应报文状态码

响应信息中的数据为明文或密文数据。

表A.20 响应信息中可能的状态码

SW1	SW2	说明
90	00	命令执行成功
61	Xx	还有 xx 字节需要返回
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	81	当前文件不是透明文件
69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效
69	85	使用条件不满足
69	86	没有选择当前文件
69	88	安全信息数据错误
6A	81	功能不支持
6A	82	未找到文件
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6B	00	起始地址超出范围
6C	Xx	Le 长度错误。'xx'表示实际长度
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

A.2.8 READ RECORD 命令

A.2.8.1 定义和范围

READ RECORD 命令读记录文件中指定的记录。

A.2.8.2 命令报文

表A.21 命令代码

代码	数值								
CLA	'00'								
INS	'B2'								
P1	记录号（'00'表示当前记录） 记录标识符（'00'按记录号顺序指定第一个、最后一个、下一个、前一个）								
P2	b8	b7	b6	b5	b4	b3	b2	b1	说 明

表 A.21 （续）

代码	数值								
	0	0	0	0	0	-	-	-	当前的 EF 文件
	x	x	x	x	x	-	-	-	用 SFI 方式
	1	1	1	1	1	-	-	-	保留
	-	-	-	-	-	1	x	x	利用 P1 中的记录号
	-	-	-	-	-	1	0	0	P1 记录号
	-	-	-	-	-	1	0	1	从 P1 到记录尾
	-	-	-	-	-	1	1	0	从记录尾到 P1
	-	-	-	-	-	0	x	x	利用 P1 中的记录标识符
	-	-	-	-	-	0	0	0	P1 指定标识的第一个实例
	-	-	-	-	-	0	0	1	P1 指定标识的最后一个实例
	-	-	-	-	-	0	1	0	P1 指定标识的下一个实例
	-	-	-	-	-	0	1	1	P1 指定标识的前一个实例
	任何其他值								保留
Lc	不存在								
DATA	不存在								
Le	期望返回的明文字节数								

A.2.7.6 命令报文数据域

命令报文数据域不存在

A.2.7.7 响应报文数据域

所有执行成功的READ RECORD命令的响应报文数据域由读取的记录组成。

A.2.8.3 响应报文状态码

表A.22 响应信息中可能的状态码

SW1	SW2	说明
90	00	命令执行成功
61	xx	还有 xx 字节需要返回
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	81	当前文件不是记录文件
69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效
69	85	使用条件不满足
69	86	没有选择当前文件
69	88	安全信息数据错误
6A	81	功能不支持
6A	82	未找到文件
6A	83	未找到记录
6A	85	Lc 与 TLV 结构不匹配

表 A.22 （续）

SW1	SW2	说明
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6C	xx	Le 错误，‘xx’表示实际长度
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

A.2.9 SELECT FILE 命令

A.2.9.1 定义和范围

SELECT FILE 命令通过文件标识或应用名来选择 IC 卡中的 MF、DDF、ADF 或 EF 文件。

A.2.9.2 命令报文

表A.23 命令代码

代码	数值
CLA	‘00’
INS	‘A4’
P1	‘00’通过 FID 选择 DF、EF ‘04’通过 DF 名选择应用
P2	‘00’ 第一个或仅有一个文件实例 ‘02’ 下一个文件实例（P1=04h 时）
Lc	若 P1=‘00’，‘02’ 若 P1=‘04’，‘05’—‘10’DATA 域的数据长度
DATA	若 P1=‘00’，FID（2 字节） 若 P1=‘04’，应用名（AID）
Le	‘00’

A.2.7.8 命令报文数据域

命令报文数据域应包括所选择的DF的AID或FID、EF的FID组成。

A.2.7.9 响应报文数据域

响应报文数据域应包括所选择DF的FCI信息。

A.2.9.3 响应报文状态码

表A.24 响应信息中可能的状态码

SW1	SW2	说 明
90	00	命令执行成功
62	83	选择文件无效
67	00	Lc 长度错误
6A	81	功能不支持

表 A.24 (续)

SW1	SW2	说 明
6A	82	未找到文件
6A	86	P1、P2 参数错
6A	87	Lc 与 P1-P2 不匹配
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

A.2.10 UPDATE BINARY 命令

A.2.10.1 定义和范围

UPDATE BINARY 命令用给定的数据代替透明文件中已有的数据。

A.2.10.2 命令报文

表A.25 命令代码

代码	数值								
CLA	'00'								
INS	'D6'								
P1	b8	b7	b6	b5	b4	b3	b2	b1	说 明
	0	x	x	x	x	x	x	x	当前 EF 文件偏移地址高字节
	1	0	0	x	x	x	x	x	通过 SFI 方式访问
P2	若 P1 的 b8=0，偏移地址低字节 若 P1 的 b8=1，偏移地址								
Lc	后续数据的长度								
DATA	写入或更新原有数据的新数据								
Le	不存在								

A.2.10.3 命令报文数据域

写入或更新的新数据。

A.2.10.4 响应报文数据域

响应报文数据域不存在。

A.2.10.5 响应报文状态码

表A.26 响应信息中可能的状态码

SW1	SW2	说明
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	81	当前文件不是透明文件
69	82	不满足安全状态
69	83	认证密钥锁定

表 A.26 （续）

SW1	SW2	说明
69	84	引用数据无效
69	85	使用条件不满足
69	86	未选择文件
69	88	安全信息数据错误
6A	81	功能不支持
6A	82	未找到文件
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6B	00	起始地址超出范围
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

A.2.11 UPDATE RECORD 命令

A.2.11.1 定义和范围

UPDATE RECORD 命令用给定的数据代替记录文件中指定的记录。对循环定长记录文件，可以通过修改上一条记录的方式实现添加记录。

A.2.11.2 命令报文

表A.27 命令代码

代码	数值								
CLA	'00'								
INS	'DC'								
P1	记录号（'00'表示当前记录） 记录标识符（P1='00'时，按记录号顺序指定第一条、最后一条、下一条、前一条）								
P2	b8	b7	b6	b5	b4	b3	b2	b1	说 明
	0	0	0	0	0	-	-	-	当前的 EF 文件
	x	x	x	x	x	-	-	-	用 SFI 方式
	1	1	1	1	1	-	-	-	保留
	-	-	-	-	-	1	x	x	利用 P1 中的记录号
	-	-	-	-	-	1	0	0	P1 记录号
	-	-	-	-	-	0	x	x	利用 P1 中的记录标识符
	-	-	-	-	-	0	0	0	P1 指定标识的第一个实例
	-	-	-	-	-	0	0	1	P1 指定标识的最后一个实例
	-	-	-	-	-	0	1	0	P1 指定标识的下一个实例
	-	-	-	-	-	0	1	1	P1 指定标识符的上一个实例
	任何其他值								保留
Lc	后续数据长度								
DATA	添加或更新原有记录的新记录								
Le	不存在								

A.2.11.3 命令报文数据域

添加或更新原有记录的新记录

A.2.11.4 响应报文数据域

响应报文数据域不存在。

A.2.11.5 响应报文状态码

表A.28 响应信息中可能的状态码

SW1	SW2	说明
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	81	当前文件不是记录文件
69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效
69	85	使用条件不满足
69	86	未选择文件
69	88	安全信息数据错误
6A	81	功能不支持
6A	82	未找到文件
6A	83	未找到记录
6A	85	Lc 与 TLV 结构不匹配
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

A.2.12 COMPUTE SIGNATURE 命令

A.2.12.1 定义和范围

COMPUTE SIGNATURE 命令用指定的私钥对数据签字。

SM2 签名不补位。

A.2.12.2 命令报文

表A.29 命令代码

代码	数 值								
CLA	'80'								
INS	'36'								
P1	b8	b7	b6	b5	b4	b3	b2	b1	说 明

表 A.29 (续)

代码	数 值								
	0	0	0	0	0	0	0	0	用当前的私钥文件
	1	0	0	x	x	x	x	x	用 SFI 指定的私钥文件
P2	SM2 签名：送入 32 字节数据								
Lc	SM2 算法：Lc='20'								
DATA	待签名数据								
Le	SM2 算法：Le='40'								

A.2.12.3 **命令报文数据域**

待签名数据。

A.2.12.4 **响应报文数据域**

签名数据。

A.2.12.5 **响应报文状态码**

表A.30 响应信息中可能的状态码

SW1	SW2	说 明
90	00	命令执行成功
61	xx	命令执行成功
67	00	Lc 长度错
69	81	文件类型不匹配
69	82	不满足安全状态
69	85	使用条件不满足
69	86	没有选择密钥文件
6A	80	数据域错
6A	81	功能不支持
6D	00	命令不存在
93	03	应用永久锁定

A.2.13 VERIFY SIGNATURE **命令**

A.2.13.1 **定义和范围**

VERIFY SIGNATURE 命令用指定的公钥对数据签字进行认证。

输入和输出数据均为高字节在前。

A.2.13.2 **命令报文**

表A.31　命令代码

代码	数　值								
CLA	'80'								
INS	'38'								
P1	b8	b7	b6	b5	b4	b3	b2	b1	说 明
	0	0	0	0	0	0	0	0	用当前的公钥文件认证
	1	0	0	x	x	x	x	x	用 SFI 指定的公钥文件认证
P2	0	0	0	0	0	0	0	0	SM2 算法
Lc	SM2 算法：'60'								
DATA	SM2 算法：待签名数据（'20'）+签名结果（'40'）								
Le	SM2 算法：无								

A.2.13.3 命令报文数据域

待签名数据和签名结果。

A.2.13.4 响应报文数据域

响应报文数据域不存在。

A.2.13.5 响应报文状态码

响应信息中的数据：无响应数据。

表A.32　响应信息中可能的状态码

SW1	SW2	说　明
90	00	命令执行成功
61	Xx	命令执行成功
67	00	Lc 长度错
69	81	文件类型不匹配
69	82	不满足安全状态
69	85	使用条件不满足
69	86	没有选择密钥文件
69	88	签名认证失败
6A	80	数据域错
6A	81	功能不支持
6A	86	P1、P2 参数错
6D	00	命令不存在
93	03	应用永久锁定

A.2.14 PKI ENCIPHER 命令

A.2.14.1 定义和范围

PKI ENCIPHER 命令用公钥加密数据。

SM2 算法不补位，可以进行 1 到 159 字节加密。

A.2.14.2 命令报文

表A.33 命令代码

代码	数 值								
CLA	'80'								
INS	'30'								
P1	b8	b7	b6	b5	b4	b3	b2	b1	说 明
	0	0	0	0	0	0	0	0	用当前的公钥文件加密
	1	0	0	x	x	x	x	x	用 SFI 指定的公钥文件加密
P2	'00' SM2 算法								
Lc	SM2 算法：'01'~'9F'								
DATA	待加密数据								
Le	SM2 算法：Lc+96								

命令报文数据域为待加密数据(高字节在前)。

SM2 算法 P2='00'，送入数据长度 0<Lc<'A0'。

A.2.14.3 命令报文数据域

待加密数据。

A.2.14.4 响应报文数据域

响应报文数据域为模长长度加密结果。

A.2.14.5 响应报文状态码

表A.34 响应信息中可能的状态码

SW1	SW2	说 明
90	00	命令执行成功
61	XX	正常处理
67	00	Lc 长度错
69	81	文件类型不匹配
69	82	不满足安全状态
69	85	使用条件不满足
69	86	没有选择密钥文件
6A	80	数据域错

表 A.34 （续）

SW1	SW2	说 明
6A	81	功能不支持
6A	82	文件未找到
6A	86	P1、P2 参数错
93	03	应用永久锁定

A.2.15 PKI DECIPHER 命令

A.2.15.1 定义和范围

PKI DECIPHER 命令用指定的私钥解密数据。

A.2.15.2 命令报文

表A.35 命令代码

代码	数 值								
CLA	'80'								
INS	'32'								
P1	b8	b7	b6	b5	b4	b3	b2	b1	说 明
	0	0	0	0	0	0	0	0	用当前的私钥文件解密
	1	0	0	x	x	x	x	x	用 SFI 指定的私钥文件
P2	0	0	0	0	0	0	0	0	SM2 算法
Lc	SM2 算法：'60'<Lc<='FF'								
DATA	待解密数据								
Le	SM2 算法：0<Le<'A0'								

A.2.15.3 命令报文数据域

命令报文数据域为模长长度待解密数据 （高字节在前）。

A.2.15.4 响应报文数据域

响应报文数据域长度为大于0且小于160。

A.2.15.5 响应报文状态码

表A.36 响应信息中可能的状态码

SW1	SW2	说 明
90	00	命令执行成功
61	80/XX	正常处理
67	00	Lc 长度错
69	81	文件类型不匹配

表 A.36 （续）

SW1	SW2	说 明
69	82	不满足安全状态
69	85	使用条件不满足
69	86	没有选择密钥文件
6A	80	数据域错
6A	81	功能不支持
6A	82	文件未找到
6A	86	P1、P2 参数错
93	03	应用永久锁定

A.2.16 GENERATE ENVELOP 命令

A.2.16.1 定义和范围

GENERATE ENVELOP 命令用指定公钥加密对称密钥，送出卡外。对称密钥为卡内产生的随机数并存在卡内临时密钥寄存器中 。该命令后可以跟 CIPHER DATA 命令，对数据加解密。若插入别的命令，密钥失效。

SM2 算法：若密钥长度为 N，被加密的临时密钥的数据结构为 ：

00 || 02 ||(32 – 3 – N) 长随机数|| 00 || 密钥数据 (N 字节) 。

A.2.16.2 命令报文

表A.37 命令代码

代码	数 值								
CLA	‘80’								
INS	‘3A’								
P1	b8	b7	b6	b5	b4	b3	b2	b1	说 明
	0	0	0	0	0	0	0	0	用当前的公钥文件
	1	0	0	x	x	x	x	x	用 SFI 指定的公钥文件
P2	‘03’ SM1 算法用卡内产生的 16 字节随机数								
Lc	不存在								
Data	不存在								
Le	SM2 算法： ‘80’								

A.2.16.3 命令报文数据域

命令报文数据域不存在。

A.2.16.4 响应报文数据域

响应报文数据域为128字节长度的信封。

A.2.16.5 响应报文状态码

表A.38 响应信息中可能的状态码

SW1	SW2	说 明
90	00	命令执行成功
61	XX	正常处理
69	81	文件类型不匹配
69	82	不满足安全状态
69	85	使用条件不满足
69	86	没有选择密钥文件
6A	81	功能不支持
6A	82	文件未找到
6A	86	P1、P2 参数错
6C	80	Le 长度错，应为 80h
93	03	应用永久锁定

A.2.17 OPEN ENVELOP 命令

A.2.17.1 定义和范围

OPEN ENVELOP 命令用指定私钥解密数字信封数据，得到对称密钥。对称密钥装入临时密钥寄存器。SM2 算法加密前的信封数据格式为：

00 ‖ 02 ‖ (32 – 3 – N) 长的随机数 ‖ 00 ‖ 密钥数据 (N 字节) 。

该命令后可以跟 CIPHER DATA 命令，对数据加解密。若插入别的命令，密钥失效。

信封数据的低字节为密钥数据的低 N 字节。

A.2.17.2 命令报文

表A.39 命令代码

代码	数 值								
CLA	'80'								
INS	'3C'								
P1	b8	b7	b6	b5	b4	b3	b2	b1	说 明
	0	0	0	0	0	0	0	0	用当前的私钥文件
	1	0	0	x	x	x	x	x	用 SFI 指定的私钥文件
P2	x	0	0	0	0	0	1	1	SM1 算法
Lc	SM2 算法： '80'								
DATA	信封数据								

表 A.39 (续)

代码	数 值
Le	不存在

A.2.17.3 **命令报文数据域**

命令报文数据域为模长长度的信封数据。

A.2.17.4 **响应报文数据域**

响应报文数据域不存在。

A.2.17.5 **响应报文状态码**

响应报文数据域不存在。

表A.40 响应信息中可能的状态码

SW1	SW2	说 明
90	00	命令执行成功
67	00	Le 长度错
69	81	文件类型不匹配
69	82	不满足安全状态
69	85	使用条件不满足
69	86	没有选择密钥文件
6A	80	数据域错
6A	81	功能不支持
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6D	00	命令不存在
93	03	应用永久锁定

A.2.18 CIPHER DATA **命令**

A.2.18.1 **定义和范围**

该命令采用对称算法对数据进行加/解密计算。对称算法类型由文件中或临时生成的指定密钥的算法决定。

该命令应使用密钥文件中的加/解密密钥或卡内临时密钥进行加/解密计算。

使用卡内临时密钥进行加/解密计算时，卡内应存在临时密钥。执行 GENERATE ENVELOP 命令或 OPEN ENVELOP 命令可以在卡内装载临时密钥。

该命令执行后，临时密钥仍然有效。

A.2.18.2 **命令报文**

表A.41　命令代码

代码	数　值
CLA	'80'
INS	'3E'

表 A. 41　（续）

代码	数　值								
P1	b8	b7	b6	b5	b4	b3	b2	b1	说 明
	0	0	0	0	0	0	0	0	用卡内的临时密钥寄存器中的密钥加/解密
	1	x	x	x	x	x	x	x	用指定密钥加/解密，bit7-bit1 为密钥标识
P2	'00'　加密								
	'01'　解密								
Lc	输入数据的长度 (对称算法分组长度的整数倍)								
Data	输入数据								
Le	返回数据长度								

输入的待加密或解密数据，数据长度应为对称算法分组长度的整数倍。

A.2.18.3 命令报文数据域

输入的待加密或解密数据

A.2.18.4 响应报文数据域

加密或解密后的结果数据。

A.2.18.5 响应报文状态码

表A.42　响应信息中可能的状态码

SW1	SW2	说　明
90	00	命令执行成功
67	00	Lc 长度错
61	xx	正常处理
69	01	该命令无效
69	81	文件类型不匹配
69	82	不满足安全状态
69	85	使用条件不满足
6A	81	功能不支持

表 A.42 （续）

SW1	SW2	说 明
6A	88	未找到密钥数据
6D	00	命令不存在
93	03	应用永久锁定

A.2.19 HASH OPERATION 命令

A.2.19.1 定义和范围

该命令采用 SHA-1、SM3 散列算法将长度小于 264 的数据分别散列处理为 20 字节、32 字节，用于签名或验证时使用。若数据总长度小于等于 64 字节（SM3 算法 192 字节），直接对该数据进行散列处理；否则以 64 字节为一块重复执行此指令，进行分块散列处理。散列处理完最后一块数据后，用 GET RESPONSE 获得 20 字节（SHA-1 算法）/32 字节（SM3 算法）/摘要结果。

A.2.19.2 命令报文

表A.43 命令代码

代码	数 值								
CLA	'80'								
INS	'34'								
P1	b8	b7	b6	b5	b4	b3	b2	b1	说明
	x	x	x	x	0	0	0	0	SHA-1 算法
	x	x	x	x	0	0	0	1	SM3 算法
	0	0	0	0	x	x	x	x	压缩数据
P2	'00' 无后续块 '01' 有后续块								
Lc	待处理数据的长度 P2='00'时，Lc<='40' P2='01'时，Lc='40'								
DATA	待处理数据								
Le	P2='01'时，不存在 P2='00'时： P1 为 SHA-1 算法时，'14' 摘要结果返回长度 P1 为 SM3 算法时，'20' 摘要结果返回长度								

A.2.19.3 命令报文数据域

命令报文数据域为待散列处理的数据。

A.2.19.4 响应报文数据域

响应报文数据域为不存在或20字节（SHA-1算法）/32字节（SM3算法）摘要结果。当有后续块时，Lc不存在，不返回数据。当是最后一块数据，返回20字节（SHA-1算法）/32字节（SM3算法）摘要结果数据。

A.2.19.5 响应报文状态码

表A.44 响应信息中可能的状态码

SW1	SW2	说 明
90	00	命令执行成功
61	XX	正常处理
67	00	Lc 长度错
6A	86	P1、P2 参数错
6D	00	命令不存在
93	03	应用永久锁定

A.2.20 SM2 KEY EXCHANGE 命令

A.2.20.1 定义和范围

SM2 KEY EXCHANGE 命令实现在IC卡内进行SM2密钥协商，得到对称密钥。对称密钥装入临时密钥寄存器。该命令后可以跟 CIPHER DATA 命令，对数据加解密。若插入别的命令，密钥失效。

A.2.20.2 命令报文

表A.45 命令代码

代码	数 值
CLA	'80'
INS	'44'
P1	'00' 表明协商过程为接收方 '01' 表明协商过程为发起方
P2	'03' SM1 算法生成 16 字节协商密钥
Lc	'88'~'C6'

表 A.45 (续)

代码	数 值	
DATA	临时公钥文件标识	1Byte
	临时私钥文件标识	1Byte
	固有公钥文件标识	1Byte
	固有私钥文件标识	1Byte
	对方的临时公钥 Gx	32Byte
	对方的临时公钥 Gy	32Byte
	对方的固有公钥 Gx	32Byte
	对方的固有公钥 Gy	32Byte
	己方 ID 长度	1Byte
	己方 ID	1-32Byte
	对方 ID 长度	1Byte
	对方 ID	1-32Byte
Le	不存在	

A.2.20.3 **命令报文数据域**

命令报文数据域为输入数据。

A.2.20.4 **响应报文数据域**

响应报文数据域不存在。

A.2.20.5 **响应报文状态码**

表A.46 响应信息中的可能状态码

SW1	SW2	说 明
61	xx	命令执行成功
67	00	Lc 长度错
69	81	文件类型不匹配
69	82	不满足安全状态
69	85	使用条件不满足
6A	80	数据域错
6A	82	未找到密钥文件
6A	86	P1、P2 参数错
6A	81	功能不支持
6D	00	命令不存在
93	03	应用永久锁定

A.2.21 SM2 GETZA **命令**

A.2.21.1 **定义和范围**

该命令辅助 SM2 签名运算，用于获得 Za 数据。

用 GET RESPONSE 获得 32 字节结果。

A.2.21.2 命令报文

表A.47 命令代码

代码	数 值
CLA	'80'
INS	'4E'
P1	'00'
P2	'00'
Lc	待处理数据的长度 '42'≤ Lc ≤'61'
DATA	待处理数据 AID 长度（1 字节）‖AID（1-32 字节）‖与 AID 匹配的公钥（64 字节）
Le	ZA 结果 Le = '20'

A.2.21.3 命令报文数据域

为待处理数据。

A.2.21.4 响应报文数据域

响应报文数据域为32字节ZA初始化结果数据。

A.2.21.5 响应报文状态码

表A.48 响应信息中可能的状态码

SW1	SW2	说 明
90	00	命令执行成功
61	XX	正常处理，
67	00	Lc 长度错
6A	86	P1、P2 参数错
6D	00	命令不存在
93	03	应用永久锁定

A.2.22 GENERATE KEY PAIR

A.2.22.1 命令描述

GENERATE KEY PAIR 命令用于生成 SM2 密钥对，根据 P2 指示的私钥文件的文件类型来决定生成 SM2 密钥对。

A.2.22.2 使用条件和安全

若要保存密钥，则应满足相应公钥和私钥文件的写条件和写属性。

若不保存密钥，则没有安全限制。

A.2.22.3 命令格式

表A.49　命令代码

代码	数　值								
CLA	'80'								
INS	'46'								
P1	b8	b7	b6	b5	b4	b3	b2	b1	说 明
	1	0	0	0	0	0	0	0	SM2 算法：返回刚生成的公钥
	1	0	1	–	–	–	–	–	SM2 算法：返回公钥和私钥，不保存
	0	X	X	–	–	–	–	–	保存公钥文件，公钥文件 SFI 为 bit5-bit1。
	–	–	–	X	X	X	X	X	指定公钥文件的 SFI。
P2	b8	b7	b6	b5	b4	b3	b2	b1	说 明
	0	0	0	–	–	–	–	–	保留。
	0	0	1	–	–	–	–	–	保留。
	0	1	0	–	–	–	–	–	保留。
	0	1	1	–	–	–	–	–	保留。

表 A.49 （续）

代码	数　值								
	1	0	0	–	–	–	–	–	保留。
	0	0	0	0	0	0	0	0	P1='A0'时
	–	–	–	X	X	X	X	X	指定私钥文件的 SFI。
Lc	不存在								
Data	不存在								
Le	不存在或可变								

A.2.22.4 响应信息

返回公钥和私钥。

表A.50　响应信息中可能的状态码

SW1	SW2	说　明
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错
69	82	不满足安全状态
6A	81	功能不支持
6A	82	未找到文件
6A	86	P1P2 参数错
67	00	长度错
6D	00	命令不存在
93	03	应用永久锁定

A.2.23 GET PUBLIC KEY 命令

A.2.23.1 命令描述

此命令只对 PKI 规范有效。

从 SM2 公钥文件中读出 SM2 公钥。

A.2.23.2 使用条件和安全

若从公钥文件中读出相应密钥参数，则需满足密钥文件的读条件和读属性。

A.2.23.3 命令格式

表A.51 命令代码

代码	数 值								
CLA	'80'								
INS	'48'								
P1	b8	b7	b6	b5	b4	b3	b2	b1	说 明

表 A. 51 （续）

代码	数 值								
	0	0	0	0	0	0	0	0	从当前的公钥文件中读取密钥 (Select File 所选)
	1	0	0	x	x	x	x	x	从 SFI 指定的公钥文件中读取密钥
P2	'01'						SM2 算法：读取公钥 Qx		
	'02'						SM2 算法：读取公钥 Qy		
Lc	不存在 (不带校验方式)								
Le	期望返回的字节数								

A.2.23.4 响应信息

读出 SM2 密钥。

表A.52 响应信息中可能的状态码

SW1	SW2	说 明
90	00	命令执行成功
61	xx	当采用校验方式时，表示正确执行 XX 表示响应数据长度。可用 GET RESPONSE 命令取回响应数据。
65	81	写 EEPROM 失败
67	00	Lc 长度错
69	81	文件类型不匹配
69	82	不满足安全状态
69	85	使用条件不满足
69	86	未选择文件
69	88	安全报文错

表 A.52 （续）

SW1	SW2	说 明
6A	81	功能不支持
6A	82	未找到文件
6A	86	P1、P2 参数错

A.2.24 STORE PKI KEY 命令

A.2.24.1 命令描述

此命令只对 PKI 规范有效。

STORE PKI KEY 命令用于将 SM2 公钥、私钥参数放入相应公钥、私钥文件中。

注：公私钥要整体覆盖，例如：如果公钥已经写入 E 和 N 并生效，覆盖此公钥需要再次写入 E 和 N 两个参数，不能单独修改 E 进行覆盖。

A.2.24.2 使用条件和安全

若将密钥参数装入相应密钥文件中，则需满足密钥文件的写条件和写属性。

A.2.24.3 命令格式

表A.53 命令代码

代码	数 值								
CLA	‘80’								
INS	‘4A’								
P1	b8	b7	b6	b5	b4	b3	b2	b1	说 明
	0	0	0	0	0	0	0	0	安装公钥或私钥到当前的文件中
	1	0	0	x	x	x	x	x	安装密钥到 SFI 指定的公私钥文件
P2	‘01’			SM2 算法：写入 SM2 公钥 Qx					
	‘02’			SM2 算法：写入 SM2 公钥 Qy					
	‘03’			SM2 算法：写入 SM2 私钥 d					
Lc	Data 域的长度								
Data	P2 = ‘01’			SM2 算法：写入 SM2 公钥 Qx					SM2 算法：32 字节
	P2 = ‘02’			SM2 算法：写入 SM2 公钥 Qy					SM2 算法：32 字节
	P2 = ‘03’			SM2 算法：SM2 私钥 d					依据公钥的模长，可变 SM2 算法：32 字节

安全报文的产生方法应符合金融应用规范。

输入密钥数据高字节在前。

A.2.24.4 响应信息

表A.54　响应信息中可能的状态码

SW1	SW2	说　明
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错
69	81	文件类型不匹配
69	82	不满足安全状态
69	85	使用条件不满足
69	86	未选择文件
69	88	安全报文错误
6A	80	数据域参数错
6A	81	功能不支持
6A	82	未找到文件
6A	86	P1、P2 参数错

A.3 相关行业命令见相关行业技术规范

社保应用命令集符合 LD/T 32 要求。

金融应用命令集符合 JR/T 0025 要求。

健康应用命令集符合《居民健康卡规范》要求。

交通应用命令集符合 DB11/T 159 要求。

附录B
（规范性附录）
北京通应用安全计算

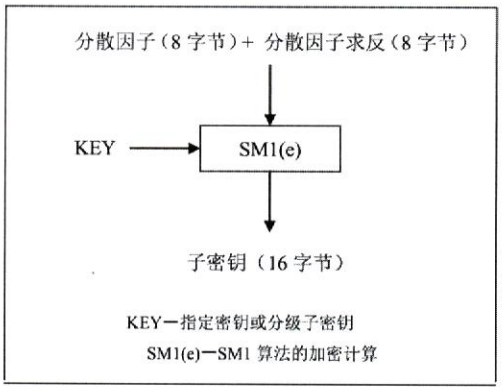
B.1 北京通应用的 SM1 算法

SM1 是以 128 位分组为单位进行运算的对称密钥算法，密钥长度为 16 字节。

B.1.1 密钥分散的计算方法

用指定的分散因子加上分散因子求反值作为输入数据，执行 SM1(e)计算，产生的 16 字节结果作为子密钥。见图 C.1。

密钥分散通过分散因子产生子密钥。

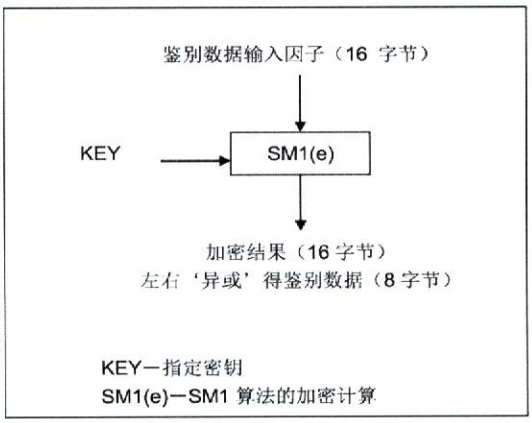


图B.1 密钥分散计算方法

B.1.2 鉴别数据的计算方法

鉴别数据的计算方法是通过对鉴别数据输入因子（16 字节）做 SM1(e)运算来产生鉴别数据，供接口设备对 IC 卡进行内部验证或外部认证，见图 B.2。。

鉴别数据输入因子由 4 字节随机数补 12 字节“000000000000000000000000”达到 16 字节构成；或由 8 字节随机数补 8 字节“0000000000000000”达到 16 字节构成；或由 16 字节随机数构成。这里 KEY 是指定密钥。

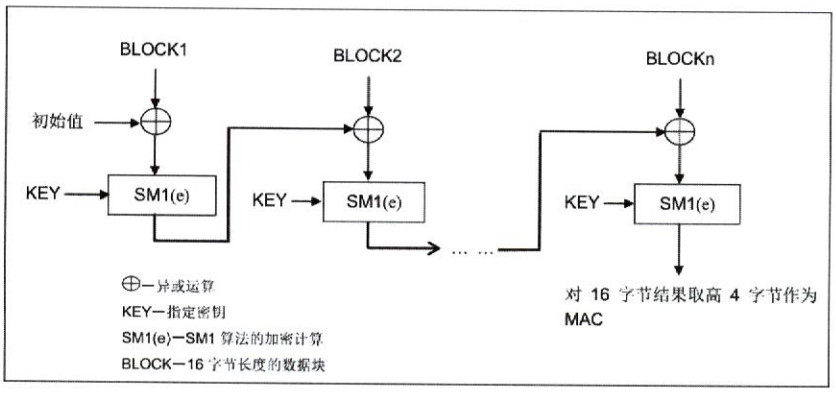


图B.2　鉴别数据的计算方法

B.1.3　安全报文中的 MAC 的计算方法

命令安全报文中的 MAC 是使用命令的所有元素（包括命令头和命令数据域中的数据）来产生的。以保证命令连同数据能够正确完整地传送，并对发送方进行认证。按照图 B.3 所示做 SM1(e)运算产生 MAC，步骤如下：

1) 取 4 字节随机数补 12 字节“000000000000000000000000”达到 16 字节作为初始值；或 8 字节随机数补 8 字节’00 00 00 00 00 00 00 00’达到 16 字节；或 16 字节随机数；
2) 将 5 字节命令头（CLA，INS，P1，P2，Lc）和命令数据域中的明文或密文数据连接在一起形成数据块。注意，这里的 Lc 应是数据长度加上将计算出的 MAC 的长度（4 字节）后得到的实际长度，Lc 的值不小于 4；
3) 将该数据块分成 16 字节为单位的数据块， 表示为 BLOCK1、BLOCK2 … … BLOCKn 等。最后的数据块有可能是 1~16 个字节；
4) 如果最后的数据块的长度是 16 字节的话，则在该数据块之后再加一个完整的 16 字节数据块‘80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00’， 转到第五步；如果最后的数据块的长度不足 16 字节，则在其后加入 16 进制数‘80’，如果达到 16 字节长度，则转到第五步；否则接着在其后加入 16 进制数‘00’直到长度达到 16 字节；
5) 按照图 B.3 所述步骤，将 16 字节运算结果取高 4 字节作为 MAC。

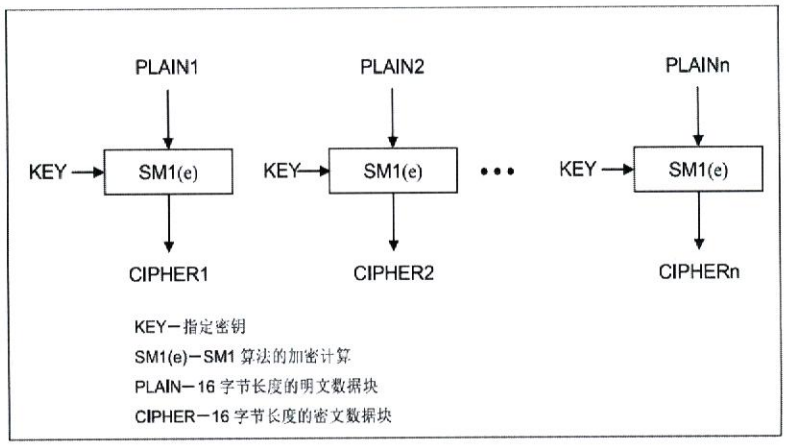


图B.3　安全报文中的 MAC 计算

B.1.4　数据加密的计算方法

安全报文传送中数据的可靠性通过对数据域的加密来得到保证。为保证命令中明文数据的保密性，可按照图 C.4 所示做 SM1(e)运算，对数据进行加密：

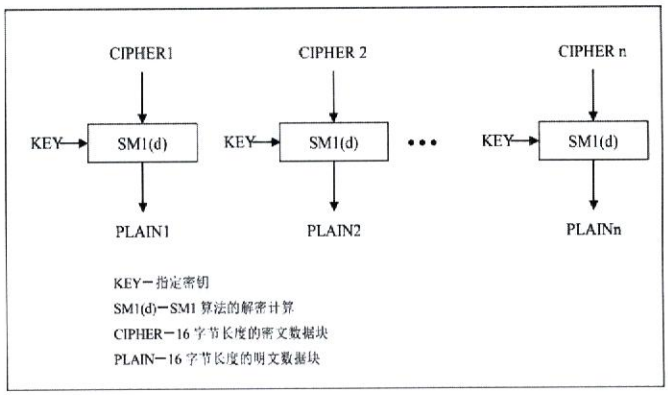
1) 用 LD（1 字节）表示明文数据的长度，在明文数据前加上 LD 产生新的数据块，LD 的值不小于 1；
2) 将该数据块分成 16 字节为单位的数据块，表示为 PLAIN1、PLAIN2 … … PLAINn 等。最后的数据块有可能是 1~16 个字节；
3) 如果最后（或唯一）的数据块的长度是 16 字节的话，转到第四步；如果不足 16 字节，则在其后加入 16 进制数‘80’，如果达到 16 字节长度，则转到第四步；否则在其后加入 16 进制数‘00’直到长度达到 16 字节；
4) 按照图 B.4 所述的算法对每一个数据块进行加密；
5) 计算结束后，所有加密后的数据块依照原顺序连接在一起。



图B.4　数据加密

B.1.5　数据解密的计算方法

数据解密与数据加密采用相反的过程，如图 B.5 所示。



图B.5　数据解密

B.2 安全报文传送的命令情况

B.2.1　CASE 1

这种情况时，命令中没有数据送到卡（Lc）中，也没有数据从卡中返回（Le）。

不含安全报文的命令：	CLA	INS	P1	P2		
含安全报文的命令：	CLA	INS	P1	P2	Lc	MAC

传送要求：　　CLA 字节的低四位应为十六进制数‘4’；
Lc = MAC 的长度，4 字节。

B.2.2　CASE 2

这种情况时，命令中没有数据送到卡（Lc）中，有数据从卡中返回（Le）。

不含安全报文的命令：

CLA	INS	P1	P2	Le

含安全报文的命令：

CLA	INS	P1	P2	Lc	MAC	Le

传送要求：　　CLA 字节的低四位应为十六进制数‘4’；
Lc = MAC 的长度，4 字节。

B.2.3　CASE 3

这种情况时，命令中有数据送到卡（Lc）中，没有数据从卡中返回（Le）。

不含安全报文的命令：

CLA	INS	P1	P2	Lc	DATA

含安全报文的命令：

CLA	INS	P1	P2	Lc	DATA	MAC

传送要求：　　CLA 字节的低四位应为十六进制数‘4’；
Lc = 数据的长度 + MAC 的长度（4 字节）。

B.2.4　CASE 4

这种情况时，命令中既有数据送到卡（Lc）中，也有数据从卡中返回（Le）。

不含安全报文的命令：

CLA	INS	P1	P2	Lc	DATA	Le

含安全报文的命令：

CLA	INS	P1	P2	Lc	DATA	MAC	Le

传送要求：　　CLA 字节的低四位应为十六进制数‘4’；
Lc = 数据的长度 + MAC 的长度（4 字节）。

附录C
（规范性附录）
北京通引用密钥分散流程

如图 C.1 所示，北京通密钥分散流程主要如下：

a) 通过密码机产生随机种子密钥并存在种子卡（CPU 卡）中，随后自定义卡片 PIN 码。初始密钥卡由四张种子卡组成。

b) 通过硬件加密机的相应加密算法，生成出北京通根密钥。

c) 根据应用代码分散出各类一级应用密钥（包括应用鉴别密钥、应用数据更新密钥、应用数据读取密钥等等）。密钥分散完成后保存在加密机中，任何人都无法以明文的形式得到密钥内容，并同时导入密钥母卡中备份保存。

d) 通过配置文件中的北京市分散因子，生成出北京市二级区域密钥，并同时导入密钥母卡中备份保存。

e) 通过硬件加密机的密钥导出功能，把各类一级应用密钥导入到 SAM 卡中，以备终端使用。

f) 在个人化发卡中心，生产制卡过程中，使用卡级分散因子与二级区域密钥进行分散，分散出每张卡片的卡级应用密钥。

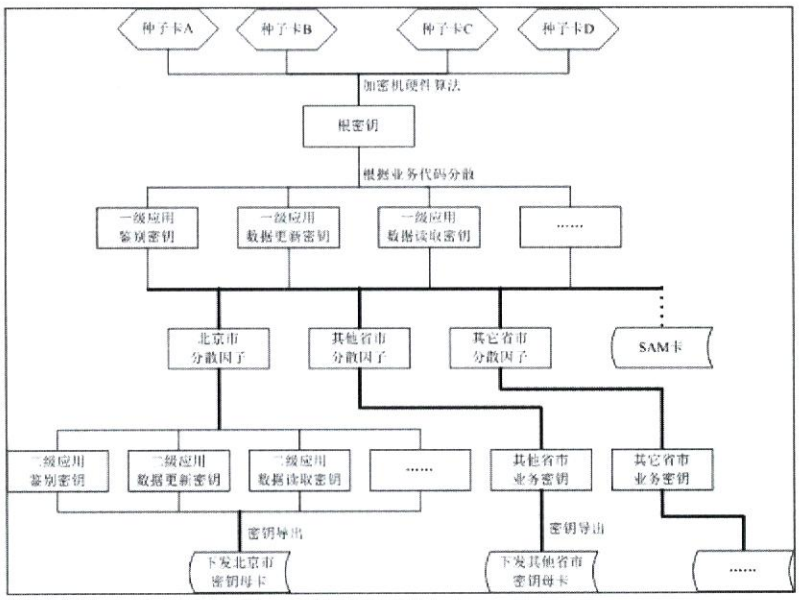


图 C.1 密钥分散流程

参 考 文 献

[1] 《居民健康卡技术规范》原卫生部 2011 年 卫办发〔2011〕60 号
[2] 《北京市社会保障卡结构说明》 北京市人力资源和社会保障局
[3] 《北京社会保障（个人）卡公钥密码应用规范》 北京市人力资源和社会保障局