ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0098.8—2012

中国金融移动支付 检测规范 第8部分：个人信息保护

China financial mobile payment—Test specifications—
Part 8: Personal information protection

2012-12-12 发布 2012-12-12 实施

中国人民银行 发布

目　　次

前言.....II
引言.....III
1　范围.....1
2　术语和定义.....1
3　基本要求.....2
4　检测细则.....7
附录A（规范性附录）　操作规程.....10
附录B（规范性附录）　判定准则.....11

前　言

《中国金融移动支付 检测规范》标准由以下8部分构成：

——第1部分：移动终端非接触式接口；

——第2部分：安全芯片；

——第3部分：客户端软件；

——第4部分：安全单元（SE）应用管理终端；

——第5部分：安全单元（SE）嵌入式软件安全；

——第6部分：业务系统；

——第7部分：可信服务管理系统；

——第8部分：个人信息保护。

本部分为该标准的第8部分。

本部分按照GB/T 1.1-2009给出的规则起草。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会（SAC/TC180）归口。

本部分负责起草单位：中国人民银行科技司、中国人民银行金融信息中心、中国金融电子化公司。

本部分参加起草单位：北京银联金卡科技有限公司（银行卡检测中心）、中金国盛认证中心、工业和信息化部计算机与微电子发展研究中心（中国软件评测中心）、上海市信息安全测评认证中心、信息产业信息安全测评中心、北京软件产品质量检测检验中心、中钞信用卡产业发展有限公司、上海华虹集成电路有限责任公司、上海复旦微电子股份有限公司、东信和平智能卡股份有限公司、大唐微电子技术有限公司、武汉天喻信息产业股份有限公司、恩智浦半导体有限公司。

本部分主要起草人：李晓枫、陆书春、潘润红、杜宁、李兴锋、张雯华、刘力慷、刘志刚、聂丽琴、李晓、尚可、郭栋、熊文韬、宋铮、李宏达、王冠华、胡一鸣、张晓、平庆瑞、张志茂、陈君、彭美玲、李微、陈吉、程恒。

引　言

随着移动支付新业务、新产品、新管理模式的不断涌现，以客户需求为主导的移动支付业务出现了不断交融和细化的趋势，不同机构之间的信息交换和信息共享变得越来越频繁。其中，个人信息在社会、经济活动中的地位日益凸显。与此同时，滥用个人信息的现象随之出现，给人民切身利益带来了危害。合理使用和有效保护个人信息已成为金融行业广泛关注的热点问题。

为了保护个人信息，促进个人信息的合理利用，在收集、分析和评估个人信息保护措施的基础上，制定本检测规范。

中国金融移动支付　检测规范　第8部分：个人信息保护

1　范围

本部分规定了移动支付个人信息保护的内部管理、组织管理、访问控制和个人信息生命周期管理4个方面的基本要求以及检测细则。

本部分适用于指导检测机构制定移动支付个人信息保护检测方案和执行检测，同时可用于指导个人信息管理机构制造相关产品和建设业务系统。

2　术语和定义

下列术语和定义适用于本文件。

2.1

个人信息　personal information

信息系统所处理、与特定自然人相关、能够单独或通过与其他信息结合识别该特定自然人的计算机数据。

本部分所涉及个人信息，包括以下部分：

a) 个人身份信息：包括个人姓名、性别、国籍、民族、证件种类号码及有效期限、职业、联系方式、婚姻状况、家庭状况、住所或工作单位地址及照片等；
b) 个人认证信息：包括在金融机构、支付机构留存的登录密码、交易密码、取款密码等；
c) 个人账户信息：包括账号、账户开立时间、开户机构、账户余额、账户交易情况等；
d) 个人信用信息：包括信用卡还款情况、贷款偿还情况以及个人在经济活动中形成的，能够反映其信用状况的其他信息；
e) 个人交易信息：包括金融机构、支付机构等在支付、结算等业务过程中获取、传输、保存的个人信息等；
f) 衍生信息：包括个人消费习惯等对原始信息进行处理、分析所形成的反映特定个人某些情况的信息；
g) 在与个人建立业务关系过程中获取、保存的其他个人信息。

2.2

敏感个人信息　sensitive personal information

一旦遭到泄露或修改，会对标识的个人信息主体造成损失或不良影响的个人信息。本部分所涉及的敏感个人信息，包括以下部分：

a) 个人身份信息：包括证件种类号码及有效期限、联系方式等；
b) 个人认证信息：包括在金融机构、支付机构留存的登录密码、交易密码、取款密码，以及预留用于找回密码的问题信息、特征码等；
c) 其他敏感个人信息：在与个人建立业务关系过程中获取、保存的其他敏感个人信息，例如个人信用信息。

2.3

一般个人信息 general personal information

个人信息中除去敏感个人信息剩余的部分。

2.4

个人信息主体 personal information subject

个人信息指向的自然人。

2.5

个人信息管理者 personal information controller

决定个人信息处理的目的和方式，实际控制个人信息并利用信息系统处理个人信息的组织和机构。

3 基本要求

3.1 个人信息管理机构内部管理要求

3.1.1 个人信息安全管理规定

应建立个人信息安全管理规定。

根据个人信息安全管理规定，提出本单位个人信息保护管理工作原则，建立内部组织管理架构，明确个人信息保护管理总体要求，并根据本单位个人信息保护管理的实际情况修订或调整有关制度。

3.1.2 个人信息安全管理操作流程

应建立个人信息安全管理操作流程。

对个人信息的访问、存储、使用、传输、加密、销毁等环节提出具体工作要求，明确各岗位在个人信息保护管理方面的工作内容。

3.1.3 个人信息安全管理权限及责任

应严格控制个人信息保护的权限管理，确保以下个人信息保护核心工作落实到岗位，责任落实到人：

a) 管理、控制对个人信息的访问权限；
b) 监控所有对个人信息的访问活动；
c) 及时处理突发个人信息安全事件；
d) 检查、监督个人信息安全管理规定的落实。

3.1.4 个人信息安全监督及检查机制

应建立日常管理监督机制，确保落实个人信息保护的各项要求。

应建立个人信息保护检查机制和工作流程，及时发现管理漏洞，确保个人信息安全。

3.1.5 个人信息安全事件应急预案

应建立个人信息保护应急预案，定期演练，及时、有效应对个人信息安全事件，降低事件造成的经济损失及不利影响。

3.1.6 个人信息安全管理审计

应定期开展个人信息保护管理相关的内部或外部审计，并根据审计结果完善相关制度、流程。

3.2 个人信息管理机构组织管理要求

3.2.1 岗位职责

应设置个人信息保护管理岗位，具体负责：

a) 制订、维护和宣传本单位个人信息保护管理制度与流程；
b) 对本单位个人信息的使用进行管理监督；
c) 对个人信息保护相关事件进行分析处理；
d) 通过技术手段保护个人信息安全。

3.2.2 人员管理

应与所有可访问个人信息的员工签署保密协议，或在劳动合同中设置保密条款。

应加强员工个人信息保护培训，确保员工了解各自岗位职责、本岗位可访问个人信息的安全等级，以及违反安全规定可能导致的后果。

员工岗位调动或离职时，应立即终止或删除该员工对个人信息的访问权限。

3.2.3 工作环境管理

应注意工作人员工作环境内所有相关的个人信息管理，防止未经授权的、无意的、恶意的使用、泄露、损毁、丢失。工作环境包括：

a) 出入管理；
b) 工作桌面；
c) 计算机接口；
d) 计算机文件系统管理；
e) 其它相关管理。

3.2.4 内部培训

应根据人员、机构、业务、需求等实际情况，制定个人信息管理相关的培训和教育制度，适时开展相应的培训。

培训的主要内容，应包括：

a) 个人信息安全相关法律、法规、规范、标准和管理制度；
b) 个人信息管理的重要性和必要性；
c) 管理、业务活动中个人信息管理的方式、措施等；
d) 违反个人信息安全相关标准可能引起的损害和后果；
e) 其它必要的教育。

3.2.5 个人信息管理文档

应在个人信息管理过程中记录与个人信息相关活动和行为的目的、时间、范围、对象、方式方法、效果、反馈等信息。这些活动和行为包括体系建立、宣传、培训教育、安全管理、过程改进、内审等。

应建立与个人信息管理相关的规章、文件、记录、合同等文档的备案管理制度，并持续改进和完善。

3.3 访问控制要求

3.3.1 基本功能

3.3.1.1 权限管理

根据“业务需要”原则，严格控制访问和使用个人信息，任何人都只能访问其开展业务所必需的个人信息，防止未经授权擅自对个人信息进行查看、篡改、泄露和破坏。

应根据“双人控制”原则，对访问权限进行分配。

3.3.1.2 身份验证

应至少采用下列一种方式验证访问个人信息的人员身份：

a) 密码；
b) 令牌（如证书等）；
c) 生物特征；
d) 其它符合要求的鉴别手段。

3.3.2 逻辑访问控制

3.3.2.1 用户账号管理

应分配唯一的用户账号给每个有权访问个人信息的用户，并采取以下管理措施：

a) 在添加、修改、删除用户账号或操作权限前，应履行严格的审批手续；
b) 对于连续 90 天未使用的账号应予以权限冻结；冻结后 30 天仍未使用的，应予以注销；
c) 用户间不得共用同一个访问账号及密码。

3.3.2.2 用户密码管理

应对用户密码管理采取下列措施，降低用户密码遭窃取或泄漏的风险：

a) 用户密码长度不得少于 6 位，应由数字和字符共同组成，不得设置简单密码；
b) 系统应强制要求用户定期更改登录密码，修改周期最长不得超过 90 天，否则将予以登录限制；
c) 应对密码进行加密保护，密码明文不得以任何形式出现；
d) 重置用户密码前必须对用户身份进行核实。

3.3.2.3 系统登录控制

系统登录服务器连续失败达到5次的，应暂时冻结该用户账号；经系统管理员对用户身份验证并通过后，再恢复其用户状态。

用户登录系统后，无任何操作时间达到或超过30分钟的，系统应要求用户重新登录并验证身份。

3.3.3 物理访问控制

3.3.3.1 机房设置电子门禁系统

机房出入口应安排专人值守并配置电子门禁系统，控制、鉴别和记录进入的人员。

3.3.3.2 来访人员申请和审批

需进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围。

3.3.3.3 设备的移入移出

存储或处理个人信息的相关设备必须在获得审批授权后方可移入或移出物理隔离区域。

3.3.3.4 对机房划分区域的管理

应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域。

3.3.3.5 重要区域设置第二道电子门禁系统

重要区域应配置第二道电子门禁系统，控制、鉴别和记录进入的人员。

3.3.3.6 监控管理

物理隔离区域进出通道均应安装录像监控设备，对人员、设备进出情况进行监控，监控录像资料至少保存90天。

3.4 个人信息生命周期管理要求

3.4.1 个人信息收集

3.4.1.1 管理要求

所有个人信息收集行为，要具有特定、明确、合法的目的，并应征得个人信息主体同意，应采用科学、规范、合法、适度、适当的收集方法和手段，以保障个人信息主体的权益。

应将收集目的、范围、方法和手段、处理方式等清晰无误的告知个人信息主体，并征得个人信息主体同意。

应只收集能够达到已告知目的的最少信息。

3.4.1.2 客户端信息收集要求

3.4.1.2.1 个人信息显示

在客户端上输入密码等敏感个人信息时，不能以明文的方式显示在屏幕上。

3.4.1.2.2 防截获

在客户端上输入个人信息时，用户输入的数据应不被移动终端的其他设备或程序非授权获取。

3.4.1.2.3 防篡改

在客户端上输入个人信息时，用户输入的数据应不被移动终端的其他设备或程序篡改。

3.4.1.2.4 防屏幕录像

客户端程序宜采用反屏幕录像技术，防范非法程序获取敏感个人信息。

3.4.2 个人信息存储

3.4.2.1 客户端信息存储要求

客户端上不能存储敏感个人信息及其密文，敏感个人信息及其密文在使用后应立即清除。

客户端存储一般个人信息时，应进行加密处理。

3.4.2.2 服务器信息存储要求

服务器存储个人信息，应根据个人信息自动和非自动处理的特点，制定相应保护策略，包括访问控制、权限设置、密钥管理等，防止个人信息的不当使用、毁损、泄露、删除等。

服务器存储敏感个人信息时，应采用加密的方式存储。

3.4.2.3 备份和恢复

应定期备份存储的个人信息，保证备份、恢复的完整性、可靠性和准确性。

3.4.3 个人信息使用

3.4.3.1 管理要求

个人信息管理者使用个人信息应基于明确、合法的目的，并遵循以下约束：

a) 应征得个人信息主体同意；或为履行与个人信息主体达成的合法协议的需要；
b) 应在个人信息收集目的范围内使用个人信息。如需要超目的范围使用个人信息，应征得该个人信息主体同意；
c) 在处理、使用个人信息时，应保证个人信息安全，保障个人信息不被任何与处理目的无关的个人、组织和机构获知；
d) 个人信息管理者向第三方提供个人信息，应获得该个人信息的个人信息主体授权，并在允许的目的范围内，采用合法、适当、适度的方法进行处理。

3.4.3.2 个人信息使用要求

敏感个人信息中的个人认证信息不能以任何形式下发到客户端。认证信息的比对只能在服务器进行。

敏感个人信息中的个人身份信息在下发至客户端之前，应屏蔽个人身份信息中不可猜测的一部分，被屏蔽部分使用统一的符号替代。

3.4.3.3 开发测试使用要求

采用专门用于测试的测试卡片进行开发测试，真实个人信息不得用于开发测试。

3.4.4 个人信息传输

3.4.4.1 管理要求

个人信息管理者传输个人信息应基于明确、合法的目的，并遵循以下约束：

a) 应征得个人信息主体同意；或为履行与个人信息主体达成的合法协议的需要；
b) 应在个人信息收集目的范围内传输个人信息。如需要超目的范围传输个人信息，应征得该个人信息主体同意；
c) 在传输个人信息时，应保证个人信息的安全，保障个人信息在传输过程中不被任何无关的个人、组织和机构获知；
d) 在传输个人信息前，应评估传输过程中可能存在的风险，明确相关责任。

3.4.4.2 通信保密性

应对传输个人信息的通信过程中的整个报文或会话过程进行加密。

3.4.5 个人信息销毁

3.4.5.1 管理要求

应制定严格的个人信息销毁制度，确保应记录个人信息的相关的文档、介质得到及时、有效的销毁。个人信息销毁前应得到相应的授权。

对于以下保存到期或已经使用完毕的个人信息，均应建立严格的销毁登记制度：

a） 纸质、光盘、磁带及其它可移动的数据存储载体等介质中存储的个人信息；

b） 报废设备或介质中存储的个人信息；

c） 其他超过保存期限需销毁的个人信息。

应保证存储敏感个人信息的介质在销毁后，信息不可恢复。

3.4.5.2 双人控制及记录

对于所有需销毁的个人信息，应在监督人员在场情况下，采取有效措施，及时妥善销毁；

对于不同类别个人信息的销毁，应分别建立销毁登记记录；销毁记录至少应包括：使用人、用途、销毁方式与时间、销毁人签字、监督人签字等内容。

4 检测细则

4.1 检测目标

检测目标是验证个人信息管理机构对个人信息保护是否符合第4章的规定，为其质量评价提供客观的依据。

4.2 检测相关规定

a） 检测操作规程见附录 A；

b） 检测判定准则见附录 B。

4.3 检测内容

个人信息保护检测项如表1所示。

表1 个人信息保护检测内容

编号	检测项		检测内容	检测项说明
1	个人信息管理机构内部管理	个人信息安全管理规定	验证是否符合3.1.1的要求	必测项
		个人信息安全管理操作流程	验证是否符合3.1.2的要求	必测项
		个人信息安全管理权限及责任	验证是否符合3.1.3的要求	必测项
		个人信息安全监督及检查机制	验证是否符合3.1.4的要求	必测项
		个人信息安全事件应急预案	验证是否符合3.1.5的要求	必测项
		个人信息安全管理审计	验证是否符合3.1.6的要求	必测项

编号	检测项			检测内容	检测项说明
2	个人信息管理机构组织管理		岗位职责	验证是否符合3.2.1的要求	必测项
			人员管理	验证是否符合3.2.2的要求	必测项
			工作环境管理	验证是否符合3.2.3的要求	必测项
			内部培训	验证是否符合3.2.4的要求	必测项
			个人信息管理文档	验证是否符合3.2.5的要求	必测项
3	访问控制	基本功能	权限管理	验证是否符合3.3.1.1的要求	必测项
			身份验证	验证是否符合3.3.1.2的要求	必测项
		逻辑访问控制	用户账号管理	验证是否符合3.3.2.1的要求	必测项
			用户密码管理	验证是否符合3.3.2.2的要求	必测项
			系统登录控制	验证是否符合3.3.2.3的要求	必测项
		物理访问控制	机房设置电子门禁系统	验证是否符合3.3.3.1的要求	必测项
			来访人员申请和审批	验证是否符合3.3.3.2的要求	必测项
			设备的移入移出	验证是否符合3.3.3.3的要求	必测项
			对机房划分区域的管理	验证是否符合3.3.3.4的要求	必测项
			重要区域设置第二道电子门禁系统	验证是否符合3.3.3.5的要求	必测项
			监控管理	验证是否符合3.3.3.6的要求	必测项
4	个人信息生命周期管理	个人信息收集	管理要求	管理要求	验证是否符合4.4.1.1的要求	必测项
			客户端信息收集	个人信息显示	验证是否符合4.4.1.2.1的要求	必测项
				防截获	验证是否符合4.4.1.2.2的要求	必测项
				防篡改	验证是否符合4.4.1.2.3的要求	必测项

编号	检测项			检测内容	检测项说明
			防屏幕录像	验证是否符合4.4.1.2.4的要求	必测项
		个人信息存储	客户端信息存储要求	验证是否符合3.4.2.1的要求	必测项
			服务器信息存储要求	验证是否符合3.4.2.2的要求	必测项
			备份和恢复	验证是否符合3.4.2.3的要求	必测项
		个人信息使用	管理要求	验证是否符合3.4.3.1的要求	必测项
			个人信息使用要求	验证是否符合3.4.3.2的要求	必测项
			开发测试使用要求	验证是否符合3.4.3.3的要求	必测项
		个人信息传输	管理要求	验证是否符合3.4.4.1的要求	必测项
			通信保密性	验证是否符合3.4.4.2的要求	必测项
		个人信息销毁	管理要求	验证是否符合3.4.5.1的要求	必测项
			双人控制及记录	验证是否符合3.4.5.2的要求	必测项

附 录 A
（规范性附录）
操作规程

A.1 基本规定

a) 检测启动应满足本标准以及其他相关规定的要求；
b) 检测机构的检测流程包括但不限于：前期准备、现场检测、综合分析、出具报告等部分。其中，现场检测包括但不限于：启动会议、中间问题沟通、最终问题确认及末次会议环节；
c) 在前期准备阶段，检测机构应向被检测机构提供检测准备清单，要求被检测机构填写情况调查表，检测机构要与被检测机构共同制定检测计划，并且双方签字确认；
d) 在现场检测阶段，检测机构对检测出的问题进行分析汇总，向被检测机构出具检测问题确认单，并且双方逐页签字确认；被检测机构要声明外包情况，并盖章后反馈给检测机构；
e) 问题确认后，经过检测机构和被检测机构协商，被检测机构可以就某些或者全部问题进行整改，并出具检测整改报告，整改后检测机构要进行回归测试；
f) 现场检测过程中要保证检测环境、系统版本稳定，一旦进入现场检测阶段，不允许再修改；
g) 被检测机构的涉密文档、核心配置等材料，检测机构要在被检测机构的制度约定下，协商查看方式、地点等。

A.2 检测方法

a) 个人信息保护检测应根据本标准的内容逐项检测，并结合对现场人员的抽查记录，进行统计分析，对相应表格的各项评价内容给出评价；
b) 个人信息保护检测的检测方法应包括但不限于：
   1) 审查相关的制度文档，检查相关的记录单据等凭证，核实制度落实情况；
   2) 与被检测机构相关人员进行访谈，询问个人信息保护相关要求，了解各项要求的执行情况；
   3) 对网络设备、主机设备以及相关应用安全配置策略的检测；
   4) 用相应工具设备或安全设备对网络、主机等设备进行扫描；
   5) 对主机操作系统上用户权限划分的检查；
   6) 对登录密码的复杂度要求、登录失败处理参数进行检查；
   7) 对数据存放位置的权限的检查；
   8) 对通信报文和会话进行抓包分析，分析报文是否采用校验或密码技术保证保密性；
   9) 对被测系统是否提供原发和抗抵赖功能进行检测，检测系统如何给出原发或接收证据；
   10) 对使用的认证技术和证书进行检查，检查服务器证书保护措施；
   11) 对使用的监控手段和设备进行核查。

附 录 B
（规范性附录）
判定准则

B.1 问题等级分类

B.1.1 严重性问题

与相关法律法规、标准规范有明显冲突；存在安全风险，会对客户利益造成严重的损害。

B.1.2 一般性问题

存在安全风险，会对客户利益造成直接或潜在的损害。

B.1.3 建议性问题

存在安全风险，但不会对客户利益造成直接或潜在的损害。

B.2 检测结果判定

B.2.1 检测项结果判定原则

a) 不符合：在检测过程中，发现严重性问题和一般性问题，该检测项的检测结果判定为“不符合”；
b) 符合：在检测过程中，未发现问题或仅发现建议性问题，该检测项的检测结果判定为“符合”；
c) 不适用：在各检测类检测过程中，根据被检测机构声明，被检测系统未提供的非必测项可判定为“不适用”。判定为不适用的检测项需说明原因和带来的安全影响。

B.2.2 检测报告结果判定原则

a) 不符合：检测项的检测结果中存在因严重问题导致的“不符合”检测项，则该检测报告的检测结果判定为“不符合”。检测项的结果中存在因一般问题导致的“不符合”检测项，如果不符合率未达到相关要求，则该检测报告的检测结果判定为“不符合”；

b) 符合：其他情况检测报告结果判定为“符合”。

参 考 文 献

[1] 银发〔2011〕17号　中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知