

移动电子政务应用 安全政务本系统手册

安全政务本技术标准联盟 主编

2015 年 1 月 北京

安全政务本技术标准联盟简介

为解决移动电子政务面临的安全和标准化问题，同时为各级政务部门的移动电子政务应用创造一套标准化的、安全的移动应用环境，国家信息中心自 2013 年 4 月起，牵头组织电信运营商及国内各平板电脑厂商，按照信息安全等级保护三级的要求设计生产了“安全政务本”，将国产平板电脑、政务 CA 证书、电信运营商数据流量卡、移动安全接入网关和移动终端管理系统集成在一起，为非涉密政务业务用户提供了一个安全、标准和集成的移动电子政务平台环境；同时牵头起草了《移动电子政务安全政务本系统安全技术要求》和《安全政务本系统测试规范》两个技术规范，经国内权威信息安全测评单位测试，各款产品符合《技术要求》要求并达到信息安全等级保护三级要求，相关产品在北京市和深圳市进行了试点试用，在国家安监总局的移动办公系统中已上线投产运行。

为进一步加强安全政务本的技术标准维护、市场宣传推广等工作，持续建立移动电子政务应用的规范化生态环境，以标准化系统来加快国内移动电子政务的应用发展，中国信息协会信息安全产业委员会组织成立“安全政务本技术标准联盟”。联盟宗旨是制定、维护、修改“安全政务本”的技术标准，宣传推广该标准，协调各参与单位进行有序的合作与竞争，以促进中国移动电子政务应用健康发展。

目录

安全政务本白皮书.....1

安全政务本系统安全技术要求.....15

运营商安全政务本办理流程.....24

FAQ.....33

安全政务本技术标准联盟成员单位.....34

安全政务本白皮书

1 安全政务本概念和特点

1.1 移动电子政务的趋势

移动通信技术的大发展推动了平板电脑的广泛应用，由于移动使用的方便性，平板电脑正在大规模地替代 PC 进入工作型应用领域。在企业界，移动终端取代 PC 成为主流终端设备已成基本趋势。在电子政务中移动终端设备大规模取代 PC 已不可避免。可以预见，不久的将来移动终端与云计算技术配套的应用模式将成为电子政务应用服务的主流。

1.1.1 重视 BYOD 的应用趋势

BYOD (By Your Own Device) 是用户使用自己的设备兼顾工作型应用与生活型应用。用户同时携带两套移动设备很不方便，因此在商务应用中 BYOD 模式已成为重要趋势。基于同样的原因，BYOD 应用模式也将会在政务应用中受到欢迎，在移动电子政务应用开发中也需要考虑使用者的这种需求，让使用者得到更多方便不仅是人性化的需求，也是提高工作效率的需要。

1.1.2 移动终端在电子政务的应用

在实际电子政务应用环境里，移动终端的应用有助于工作人员摆脱工作位置的束缚，能够更充分地利用时间，提高工作效率。

(1) **领导干部应用：**领导干部出差、开会、深入基层等活动经常会耽误文件的审批、会签等工作，移动办公系统有助于实现随时办公，提高工作效率。移动终端成为领导干部现场办公的重要工具，与政务云平台连接的移动终端为领导者提供了强有力的信息利用能力和通信能力，帮助领导干部有效处理现场问题，提高办公效率。

(2) **现场工作应用：**移动终端的使用可以使政府的许多工作实现上门服务，移动终端系统能够帮助公务员现场管理、现场执法。智能移动终端能够提升现场工作的效率，提升现场公务员的信息能力，提高现场问题处置的质量。移动终端也是现场调查的有效工具。

与 PC 终端比较，平板电脑的成本更低，使用更加简单，容易专业化和标准化，出现故障的机会也更少，移动终端在政务部门的普及已成必然趋势。

1.2 移动电子政务的信息安全

企业移动终端应用普及，其信息安全技术已经能够支持大多数企业的信息安全需求，即使是对信息安全高度敏感的企业，如金融部门也已经越来越多地利用移动终端设备提高服

务效率，说明目前移动终端系统的信息安全技术已达很高水平。

然而，电子政务移动办公却相对滞后，其重要原因是未能对政府的涉密信息与非密信息、涉密信息与敏感信息有效区分。电子政务绝大部分业务都可以在信息安全等级保护三级水平的环境下安全地运行。

将企业已成功应用的移动信息安全技术应用于电子政务业务中是大势所趋，很多政务部门已开始这方面的试验，但是还没有系统的标准和适合政务应用的规范化产品，这也影响移动电子政务应用的普及。

1.3 安全政务本概念的提出

在推广移动电子政务应用过程中，标准化的系统将因以下优势而形成移动电子政务的主流：

（1） **提高信息安全水平，促进互联互通。** 标准化的信息安全系统是诸多技术提供商共同开发维护的结果，经过了大量应用检验，其信息安全水平与应用可靠性是小范围应用系统所难以达到的。采用标准化的移动电子政务系统也有助于数据共享、系统互联互通，有助于应用技术的相互学习交流。

（2） **加快应用系统建设进度。** 用户不需要自己去找设备供应商、通信运营商、终端管理软件供应商，也不需要设计信息安全测试方案，在已有标准化应用平台上部署应用系统也会容易得多。应用系统会更有效、更安全，成本也更低。

（3） **促进移动电子政务软件与服务的消费。** 成功的软硬件可在更多部门中推广，标准化的应用平台有利于促进移动电子政务软件与服务的消费，优化电子政务的应用环境，提高政务效率。

（4） **有利于供应商提高质量，降低成本。** 标准化的技术平台容易形成产业规模，使供应商能够集中精力、积累经验、不断改进，提高系统的安全性能，提升服务效能、降低系统建设与服务的成本。

安全政务本就是一套具有以上优势的标准化系统，它由“安全政务本技术标准联盟”组织国家信息中心、中国移动、中国联通、中国电信、华为、中兴、联想和壹人壹本等单位共同设计而成。该系统在北京市、深圳市进行了电子政务业务的实际应用试点，在国家安监总局的移动办公系统中已上线投产运行。。

安全政务本在概念上是一套完整的移动电子政务系统集成技术标准（见《移动电子政务安全政务本系统安全技术要求》），安全政务本产品是指通过了国家权威信息安全检测部门测试符合上述标准的集成系统产品，该产品简称为“安全政务本”。

1.4 安全政务本主要特点

安全政务本系统具有如下特点：

- **集成化系统**

安全政务本是一个集成化的系统，它集成了成熟的移动终端（PAD）、电信运营商的通信渠道、数字证书、移动终端管理系统（MDM），形成了一个完整的移动电子政务办公环境，有效降低应用系统集成的工作量，便于各级政务部门使用。

- **标准化系统**

安全政务本有几种不同的集成版本，这些版本都符合一致的信息安全标准和互操作标准，使得安全政务本成为电子政务应用的标准化平台，有利于政务应用软件与服务的共享与销售（如 APP STORE 市场）。

- **按照信息安全等级保护要求设计与测试**

安全政务本系统方案按照等保三级的要求设计，并经过中国软件评测中心等权威机构安全测试认可。经过严格测试的系统有助于提高应用系统的信息安全保护水平。

1.5 安全政务本的应用价值

安全政务本通过安全合理的设计和测试，实现以下功能目标：

- **达到等保三级安全标准**

按国家信息安全等级保护三级标准设计，由信息安全权威机构检测，提升了信息安全的可信度；

- **方便用户应用系统集成**

安全政务本提供完整的移动电子政务配套标准，方便使用单位集成本单位的移动办公系统，甚至可由第三方按标准统一完成集成和部署；

- **便于政府采购**

移动终端设备与终端安全管理软件均可以采用租赁方式，政府购买服务，不形成固定资产；

- **统一的 APP 平台**

为政府电子政务应用创造标准化的 APP 平台，促进电子政务服务 App 的发展与共享；标准化的应用环境有利于系统的互联互通。

- **利用企业已有的成熟技术**

移动终端的先进技术商业市场应用往往快于政府应用，安全政务本是由企业界共同提出的标准，有助于市场上先进技术尽快引入电子政务应用。

1.6 政府主管部门的积极支持

安全政务本系统在工信部信息化推进司等有关部门要求和大力支持下，由国家信息中心、通信运营商、设备生产商等企业共同设计而成，能广泛应用移动电子政务领域的标准化系统。

1.7 有关部门与企业的积极配合

为进一步加强安全政务本的技术标准维护、市场宣传推广等工作，国家信息中心、中国软件评测中心、中国移动、中国电信、中国联通、华为技术有限公司、中兴通讯股份有限公司、联想集团、北京壹人壹本信息科技有限公司、北京国信灵通公司等共同成立“安全政务本技术标准联盟”（以下简称“联盟”）。

联盟致力于建立移动电子政务应用的规范化生态环境，以标准化系统来加快移动电子政务的应用发展。

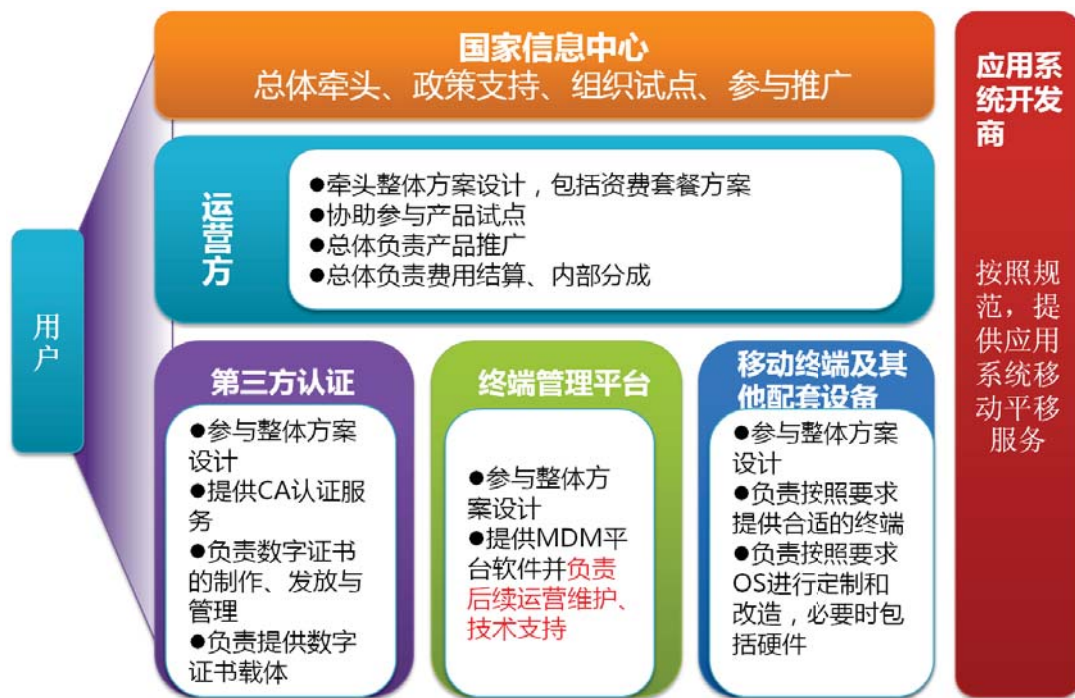


图 1 安全政务本成员架构

2 安全政务本信息安全架构

2.1 系统框架

根据移动政务的现实需求，从安全角度出发，对安全政务本系统进行详细的设计。安全政务本整体系统框架主要包括基础资源、移动设备、政务移动服务支撑和移动应用等内容，见下图。

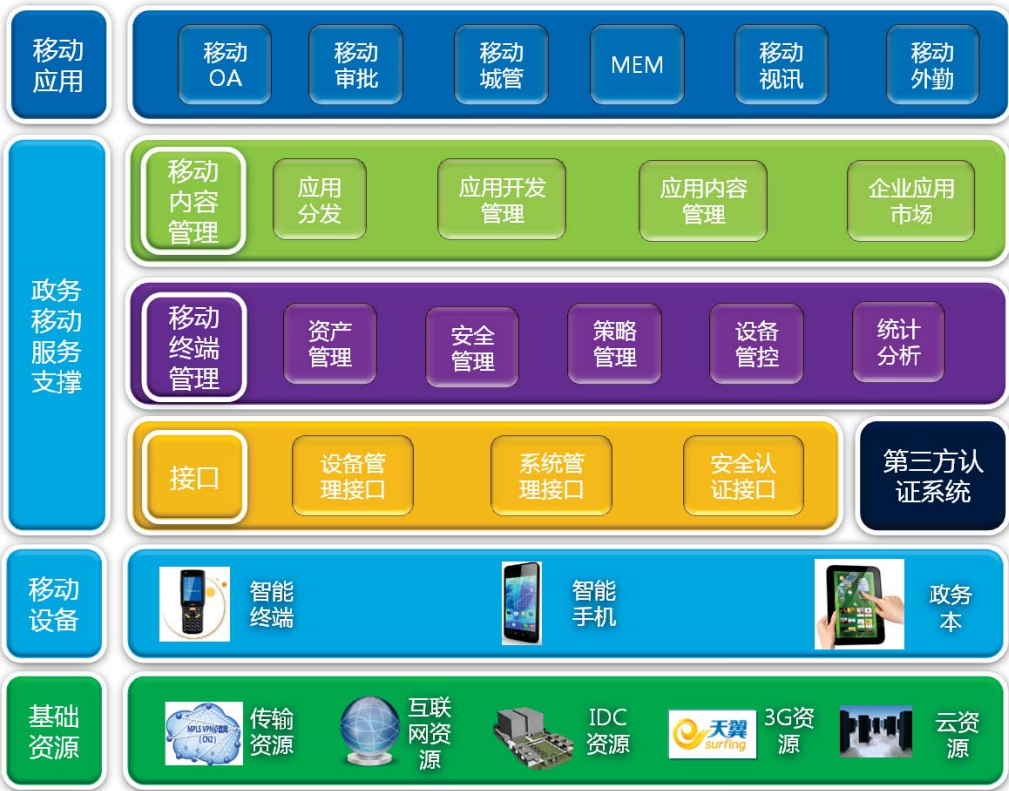


图 2 安全政务本系统框架

2.2 整体安全框架

安全政务本系统安全框架主要包括：终端安全、接入传输安全、终端集中安全管理、应用安全等四个方面，保证端到端的电子政务应用安全。

- 终端安全模块通过TF密码卡、终端安全加固、终端管理软件及安全沙箱, 实现安全政务本的终端安全、网络安全、应用安全和数据安全；
- 接入传输安全采用VPN安全加密方式或者运营商移动专用通道（APN）方式实现；
- 终端集中安全管理由安全政务本服务管理平台实现，为政务应用提供统一门户界面及应用商店，基于安全沙箱运行电子政务应用，并通过应用与用户主账号关联，可提供政务应用单点登录功能；
- 安全政务本可只安装政务应用软件，或者混合安装政务及个人应用软件。安全政务本的设计需要考虑政务与个人应用软件数据的安全隔离。

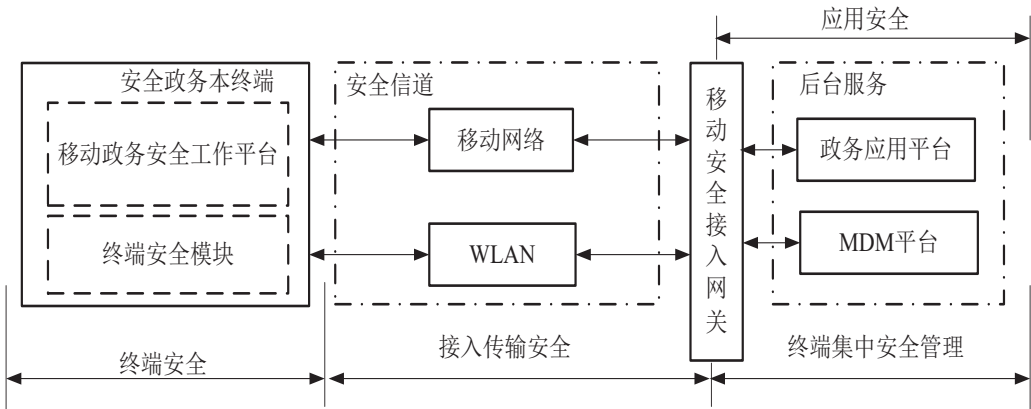


图 3 安全政务本整体安全框架

2.3 移动安全接入逻辑架构

安全政务本保障移动应用的安全接入，具体安全保障接入逻辑架构如下：

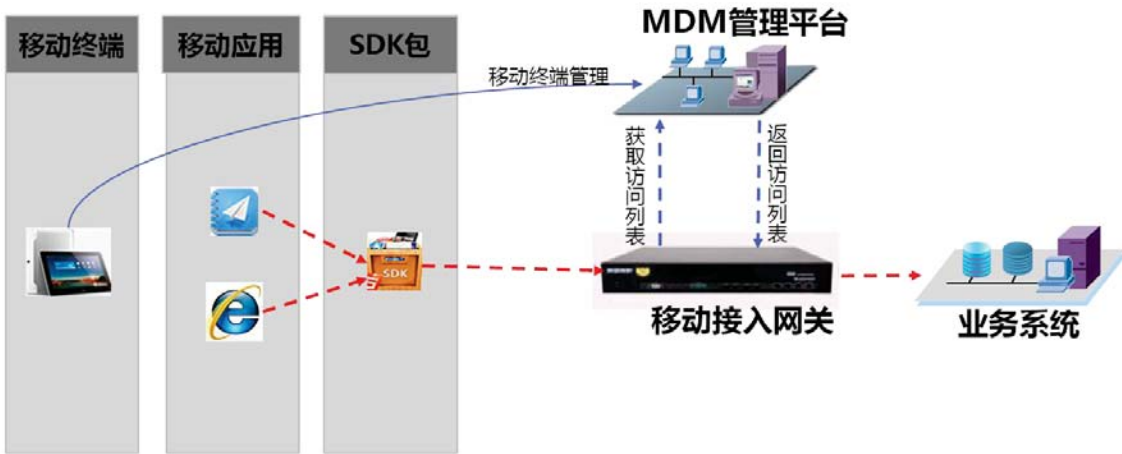


图 4 安全政务本安全接入逻辑架构

3 移动终端管理系统 (MDM)

3.1 移动终端管理内容

移动电子政务应用最复杂的问题是移动终端管理，由于移动终端的可移动性及可以与非业务应用使用同一设备（BYOD 模式）给信息安全工作增加了许多复杂性，因而需要设置专用系统来监督管理每一台终端的安全应用问题，这就是终端管理系统 MDM 的任务。

MDM 的主要功能包括用户自主服务、应用管理、设备管理、资产管理、安全管控、数据管理、后台服务等内容。

①用户自助服务	②应用管理	③设备管理	④资产管理	⑤安全管控	⑥数据管理	⑦后台服务
数据远程擦除	政务应用商店	安全策略远程下发	资产注册	准入检查	整机数据擦除	WEB策略管理
终端远程锁定	应用后台管理	远程解锁锁定	资产注销	接入认证	恢复出厂设置	安全网关集成管理
终端消息发送	应用黑白名单	ROOT检测策略	设备信息列表	远程锁定	办公数据擦除	管理信息加密传输
终端铃声提示	应用列表查询	终端密码策略	设备详细信息	GPS定位		
		硬件模块禁用策略	消息推送	远程卸载管理应用		
		合规策略判定	设备生命周期管理	证书身份绑定		

图5 移动终端管理平台（MDM）主要功能

3.2 用户自建终端安全管理系统（MDM）

安全政务本系统强调移动终端管理系统（MDM）与移动终端、通信信道、数字证书捆绑在一起提供。其中移动终端、通信信道、数字证书是容易根据用户数目采购的，开始可以小规模采购，随用户增加而逐步扩展，唯有移动终端管理系统（MDM）是需要整体购置的，初始成本较高，管理维护也比较复杂，是移动电子政务推广的难点。用户可以自建本单位的MDM系统，目前华为、中兴、中国移动、国信灵通均有成熟的产品可提供。

此外用户也可以租用已建成的MDM云系统来完成MDM管理。目前正在建设的MDM云服务有以下几个渠道：

3.3 国家信息中心的MDM管理云

为推动安全政务本的应用，国家信息中心在政务外网平台上将建立安全政务本MDM云服务平台，以支持有关政府部门的移动电子政务终端安全管理。

国家信息中心的MDM云能够方便地用于各级政府部门的移动办公试点。将电子政务的应用迁移到移动终端上并不是一件容易的事情，为稳妥起见，很多部门希望能够从小规模试点开始适应新环境的管理，此时利用国家信息中心提供的MDM云平台最为方便，在小范围的应用取得经验再制定规模化应用的方案，部门规模化应用可根据需要自建MDM管理系统，也可以扩展规模继续租用国家信息中心的MDM云实现全业务的移动终端安全管理。

MDM云服务平台向机构用户提供完整的MDM管理工具，由用户自己利用该工具自行管理本系统终端，MDM云服务提供者只保证云系统的可靠服务，并不介入用户单位的终端管理，以保障用户管理的私密性。

3.4 运营商的MDM管理云

为推广移动电子政务的应用，国内三大运营商均制定了提供全套服务的计划，不仅提

供了专用信道上的套餐优惠，还将提供终端设备配套（如预置通信卡、数字证书）服务，运营商还将提供相应的 MDM 云服务或帮助机构用户配套自用的 MDM 系统。

从长远应用考虑，运营商建立移动终端管理系统（MDM）云平台会给移动电子政务的用户，尤其是小规模的用户带来更多方便。运营商建立 MDM 云平台，与其遍布全国的服务网点相结合是推广移动电子政务的重要渠道，尤其在基层电子政务的应用普及中会起到重要作用。

4 移动电子政务标准化建设

4.1 信息安全标准化的重要性

信息安全标准制定很重要，同时维护与推广更重要。安全政务本技术标准的推行是移动电子政务推广应用的重要措施，有利于提高信息安全水准、提高建设效率、提高互操作能力、有助于应用服务标准化、有利于长远发展。

该标准由安全政务本技术标准联盟共同制定而成。联盟是一个非营利民间组织，由相关企事业单位自愿组成。联盟的宗旨是制定、维护、修改安全政务本的技术标准（技术标准重大修改需由联盟单位联席会议通过），宣传推广该标准，以促进中国的移动电子政务应用。

4.2 国家政务外网平台促进移动电子政务标准化

为提高政务外网横向、纵向覆盖率，切实解决政务应用接入“最后一公里”难题，建设和推广安全政务本是外网平台延伸发展计划的重要组成部分。同时，建立在安全政务本基础之上的 App 应用也是促进电子政务标准化发展的一个不可或缺的环节。

安全政务本标准将得到联盟的长期维护、升级、改造等。

4.3 从事实标准向国家标准的过度

在有关部门的支持下，安全政务本标准将向国家标准发展。

5 安全政务本与电子政务业务的融合

安全政务本产品重点是保障移动应用时的信息安全性，具有基本的移动办公功能，能够应对常规的办公需求，对于各级政务部门的个性化应用而言，它只是一个可以承载多样化的业务应用的通用平台，需要用户进行适应性调整。安全政务本系统具有很强的适应性，能够方便地连接用户已有的业务或开发新的应用。

5.1 业务系统的迁移

安全政务本是一个标准化的移动电子政务平台，应用规模越大，积累的经验越多，其适应新应用的能力也就越强，不仅有助于提高新应用拓展的效率，还有助于减少故障。标准

化的移动电子政务平台也有助于不同地区移动电子政务业务的相互学习,有助于软件系统的迁移。

政务应用系统向安全政务本的迁移需要进行适配。适配内容主要如下:

◆ 证书验证: 政务应用访问政务网内部系统时, 必须经过 CA 数字证书和登录密码进行双因子认证, 应通过证书与用户主账号关联, 提供单点登录功能;

◆ 安全 SDK 集成: APP 通过安全政务本管理平台提供的安全 SDK 进行应用开发集成, 实现电子政务移动办公应用的快速、安全开发、部署及应用;

5.2 基本移动办公应用

安全政务本可广泛应用于电子政务的各个领域, 例如:

- 移动办公: 利用移动终端上的软件系统, 建立与后台应用系统的联系, 摆脱时间和场所局限, 随时随地进行随身化的管理、沟通和业务处理等, 有效提高工作效率。
- 移动执法: 利用结合现代移动终端技术、移动通讯技术、GIS 技术、GPS 技术形移动执法系统, 通过装载到移动终端上, 系统执法人员可以进行拍照、摄像、录音、GPS 定位、查看法律法规、查询被监督单位信息、查看任务和通知、现场打印罚单、打印执法文书等操作。
- 移动决策: 利用无线网络技术, 结合决策信息系统而形成决策支持信息移动决策应用。
- 移动应急: 通过移动终端, 在现场进行应急事件处理。
- 移动流媒体: 在移动终端上实现的视频播放等功能。

5.3 政务外网平台通过安全政务本向基层延伸应用

国家政务外网平台的服务将向基层延伸, 为解决“最后一公里”问题、提高外网的纵向、横向覆盖率, 安全政务本的推广应用将是延伸服务的重要组成部分。

5.4 政务外网部署终端移动管理 (MDM) 云平台

业务移动设备有更大的丢失风险, 安全政务本要求政务数据只保存在服务器端, 不允许下载到移动终端内是出于信息安全的考虑。在国家政务外网平台上部署安全政务本的终端管理 (MDM) 云平台服务系统, 将统一支持政府部门委托的 MDM 管理, 加强信息安全建设。

这种数据管理模式对于政务数据的云端统一管理是一个重要的铺垫, 未来的政务数据应用将更多地采用“云平台——数据中心——移动终端”的结构, 安全政务本的应用可以结合云平台——数据中心一起推动, 将加快政务云的建设。

5.5 建立政务服务 (App) 云平台

在国家政务外网平台上建立政务服务 (App) 云, 支持各级政府的服务业务。标准化的安全政务本推广应用对于电子政务业务的规范化管理有很多好处, 强大的移动终端管理系统

(MDM) 能够有效地提升移动终端应用的一致性，用户端的软件可以更方便地推送与更新，以保持移动终端软件环境的统一。

5.6 应用案例

● 北京试点

安全政务本北京市试点工作由北京市经信委组织，北京市信息资源管理中心实施，东城、海淀、顺义、平谷等区县，城管局、高级法院等委办局参与。其解决移动办公、移动执法、移动决策、移动流媒体等移动化业务需求。

● 深圳试点

安全政务本深圳市试点工作深圳市经信委组织，深圳市电子政务资源中心实施，福田等区县，办公厅、经信委等委办局参与。其解决移动办公、移动决策等移动化业务需求。采用国家信息中心“政务 CA”证书。

● 安监移动业务

国家信息中心已与安监总局就电子认证应用和安全政务本签署战略合作协议，其中安全政务本在安监总局有三个应用方向：1) 移动办公，为领导服务，目前已上线应用；2) 移动执法，为安监系统执法工作人员服务；3) 企业自查终端，为企业巡检、设备检修提供服务。

6 信息安全的检测

6.1 安全政务本的检测标准

安全政务本的技术标准文件《移动电子政务安全政务本系统安全技术要求》和《移动电子政务安全政务本系统测试规范》由联盟制定。

6.2 安全政务本的架构检测

由联盟委托的信息安全测评机构对按标准开发的每套标准化系统进行产品测试，系统安全性能达到要求的才能获准使用安全政务本的名称。

6.3 安全政务本的应用系统检测

对于用户使用了安全政务本，部署了本部门的政务应用业务之后的移动电子政务系统，可依据使用单位的需求，由联盟推荐的信息安全测评机构进行安全测试。

安全政务本系统同时是一个移动电子政务软件工具与信息服务的共享与销售平台，为保证该平台提供的软件与服务的安全性，凡进入该平台共享或销售的软件与服务产品都需要进行信息安全评测，评测标准由安全政务本技术标准联盟制定，评测工作由联盟推荐的信息安全测评机构进行安全测试。

6.4 安全政务本的运行监测

使用了安全政务本系统的用户，为防止系统长期使用中因各种原因产生的信息安全漏洞，可委托联盟推荐的信息安全测评机构进行系统的信息安全年检。

6.5 安全政务本的检测与监测机构

目前为中国软件评测中心。

7 安全政务本系统的选购

7.1 平板电脑供应商的选择

目前安全政务本终端有如下供应商：

华为、中兴、壹人壹本、联想、中国移动。

7.2 MDM 供应商的选择

目前可供选择的 MDM 系统供应商为：

中国移动、国信灵通、华为、中兴、

凡符合安全政务本标准的终端（平板电脑）均能与上述 MDM 系统适配。

7.3 通信运营商的选择

可供选择的运营商有中国移动、中国联通和中国电信，他们均能够提供与上述符合安全政务本标准的移动终端（平板电脑）及 MDM 系统适配。

中国移动、中国电信、中国联通都参加了北京市移动电子政务试点。

7.4 数字证书的选择

数字证书需要与安全政务本进行适配并完成规范测试。目前国家政务外网管理中心运营的“政务 CA”的数字证书已完成了所需要的适配与测试工作，用户若使用该 CA 颁发的证书不需要任何适配工作，“政务 CA”证书为安全政务本的默认数字证书。

7.5 安全政务本系统的集成与采购

安全政务本系统的集成与采购可以有多种方式：

（1） 用户自己集成采购

由用户自己集成采购安全政务本系统，集成内容包括：平板电脑、运营商信道服务、数字证书、MDM 管理系统设施或 MDM 云服务，有关设施与服务必须在安全政务本标准联盟确定的供应商范围中进行选择，这样才能顺利地集成并能够达到等保三级的信息安全标准要求。用户需要分别与相关供应商洽谈价格与交付方式，为保证用户系统达到所需要的信息安全标准，建议委托权威的检测机构进行全系统安全检测。

（2） 向运营商租赁

中国移动、中国联通、中国电信等电信运营商将组织全套的安全政务本租赁服务，由

运营商提供平板电脑、信道服务、数字证书以及 MDM 云平台服务，用户可直接与有关运营商洽谈具体的租赁价格与服务内容。

运营商租赁模式简单、方便，尤其适合于小规模移动电子政务应用。

(3) 第三方代理服务

由于安全政务本系统组建涉及多方面设施与服务的集成，安全政务本技术标准联盟将批准一些有技术基础的机构提供第三方代理服务。代理机构帮助用户机构集成采购相关设施和服务，服务内容包括帮助用户选择平板电脑、联系运营商的信道服务、选择 MDM 系统或提供 MDM 云服务。

考虑到大多数用户还不熟悉安全政务本系统的应用效果，初期的第三方代理重点是为用户提供小规模 MDM 云服务，待取得一定经验之后，再帮助用户建设规模化的应用系统。

联盟可提供相关的代理与咨询服务。

7.6 其它配套服务

安全政务本产品是一个集成化的产品，需要完成智能终端、通信卡、数字证书和移动终端管理系统（MDM）的装配工作，对用户而言是一项负担。

部分终端设备供应商自己提供系统装配服务，部分设备供应商委托第三方专业服务公司完成集成、装配、检测、发货服务。

部分运营商可借助其服务网点完成如上工作，如中国联通可帮助使用联通公司通信卡的用户完成安全政务本系统产品的装配交付服务。

用户也可自行组织订货装配，为保证系统安全质量，建议用户委托安全政务本标准联盟认可的权威信息安全检测部门进行检测，以确保达到安全政务本系统的标准要求。

8 安全政务本标准与品牌的维护

8.1 安全政务本证书的颁发

通过安全政务本标准测试的系统将发给证书，证书由两部分组成，一部分说明该系统符合安全政务本标准，另一部分说明该系统达到国家信息安全等保三级的标准。证书由安全政务本标准联盟、中国软件评测中心联合签发。

8.2 安全政务本标准的维护

安全政务本的技术标准、测试标准将由安全政务本标准联盟进行维护，联盟将每半年进行一次维护修改完善工作，以保证标准能够跟上不断发展的技术与应用需求。

安全政务本技术联盟办公室设在国家信息中心信息与网络安全部，安全政务本技术标准维护宣传的日常工作由联盟办公室承担。

8.3 安全政务本品牌的使用

安全政务本既是一套技术标准，同时也是一种高质量产品的品牌。只有通过了权威信息安全测评机构评测的产品才可以获准使用“安全政务本”品牌，未经测试或测试未通过的产品不得使用“安全政务本”品牌。品牌使用授权须经联盟联席会议批准。

9 引用与参考文件、术语定义

9.1 参考文件

1. 《移动电子政务安全政务本系统安全技术要求》
2. 《移动电子政务安全政务本系统测试规范》

9.2 术语定义

● 安全政务本

安全政务本是指能够安装和运行政务应用软件，并能安全接入政务网络和访问政务应用的移动智能终端的技术标准。

安全政务本通常具备如下一种或多种典型特征：

- 1) 符合相关等级保护的安全要求；
- 2) 采用数字证书加固系统安全；
- 3) 具备终端数据加密保护；
- 4) 提供安全信道的连接；
- 5) 可以安装下载政务应用；
- 6) 具备无线通讯功能，包括移动通讯、WLAN、蓝牙等。

安全政务本也成为符合上述标准的移动智能终端系统的品牌。

● 双因子认证

双因子认证是指结合密码以及实物（如TF卡）两种条件对用户进行认证的方法。

● 缩略语

CA Certification Authority 认证中心

CRL Certificate Revocation Lists. 证书撤销列表

EAS Exchange Active Sync Microsoft Exchange 同步协议

HDMI High Definition Multimedia Interface 高清晰度多媒体接口

MDM Mobile Device Management 移动设备管理

OCSP Online Certificate Status Protocol 在线证书状态协议

OTA Over the Air Technology 空中下载技术

SDHC Secure Digital High Capacity 大容量SD存储卡

SIM Subscriber Identity Module 客户识别模块

SSL Secure Sockets Layer 安全套接层

TLS Transport Layer Security 传输层安全

VGA Video Graphics Array, 视频图形阵列

VPN Virtual Private Network 虚拟专用网

WLAN Wireless Local Area Network 无线局域网

WAPI Wireless LAN Authentication and Privacy Infrastructure 无线局域网鉴别和保密基础结构

安全政务本系统安全技术要求

1 范围

本标准提出了安全政务本系统的整体安全框架，规定了终端安全、接入传输安全、终端集中安全管理和应用安全等技术要求。

本标准适用于指导安全政务本系统的研发、生产、建设及应用等工作。

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/T18336-2008	信息安全技术	信息技术安全性评估准则
GB/T 20269-2006	信息安全技术	信息系统安全管理要求
GA/T 671-2006	信息安全技术	终端计算机系统安全等级技术要求
GB/T 25068.4	信息安全技术	远程接入的安全保护
GB/T 25068.5	信息安全技术	使用虚拟专用网的跨网通信安全保护

3 术语、定义及缩略语

3.1 术语和定义

3.1.1 安全政务本

安全政务本是指能够安装和运行政务应用软件，并能安全接入政务网络和访问政务应用的移动智能终端。

安全政务本通常具备如下一种或多种典型特征：

- 1) 符合相关等级保护的安全要求；
- 2) 采用数字证书加固系统安全；
- 3) 具备终端数据加密保护；
- 4) 提供安全信道的连接；
- 5) 可以安装下载政务应用；

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/735204144233011324>