安全政务本白皮书

安全政务本技术标准联盟

二零一四年七月

一、 移动电子政务的大趋势

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。

1.2 移动终端在电子政务的应用

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。

1.3 移动电子政务与信息安全

移动终端在商业领域应用已十分普及，企业应用移动终端同样也有信息安全问题，目前的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。

电子政务移动办公滞后的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。

1.4 移动电子政务标准化的作用

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） **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。

（2） **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。

（3） **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。

1.5 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。

二、 概念和特点

安全政务本是一套移动电子政务应用的标准化系统，由安全政务本技术标准联盟组织有关华为、中兴、联想和壹人壹本等设备生产商、中国联通、中国电信等通信运营商等企业共同设计而成。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。

2.1 概念

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”。

2.2 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。

2.3 功能目标

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：

- 除安全之责：按等保要求设计，由信息安全权威机构检测；
- 免集成之累：由第三方按标准统一完成集成和部署；
- 解炒作之忧：设备租赁方式，政府购买服务，不形成固定资产；
- 统一的 APP 平台：为应用 APP 创造成熟环境；
- 利用企业已有的成熟技术：便于快速市场化推广。

三、 系统架构

3.1 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。

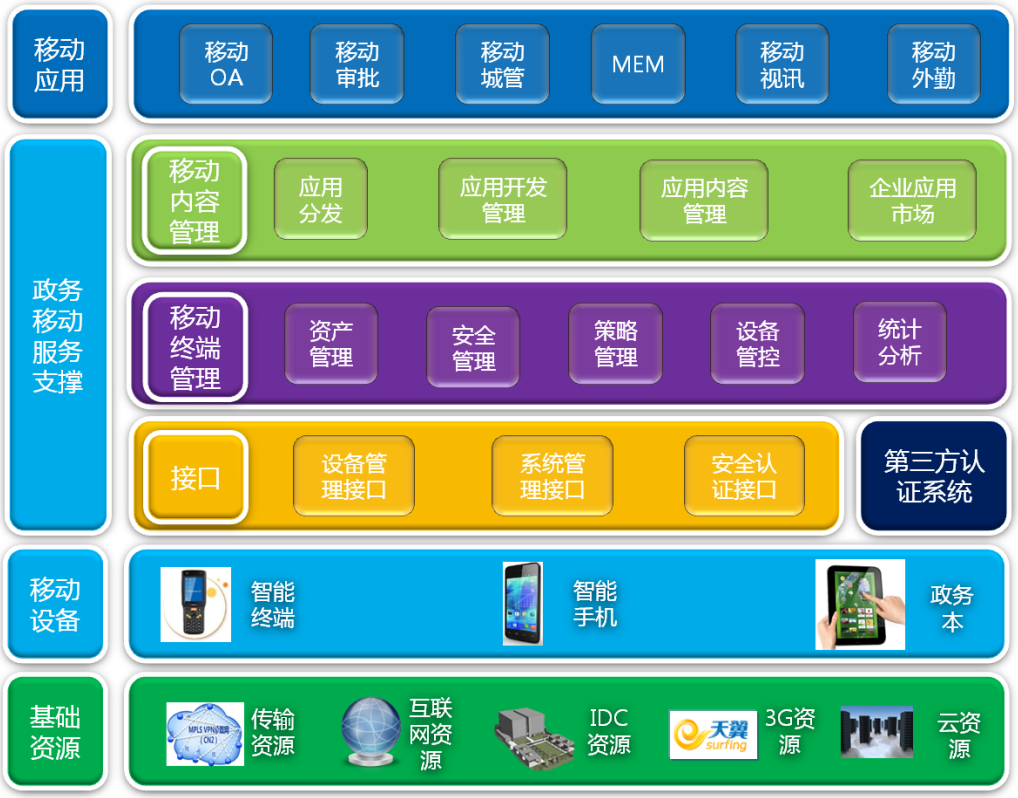

图 1 安全政务本系统框架

3.2 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。

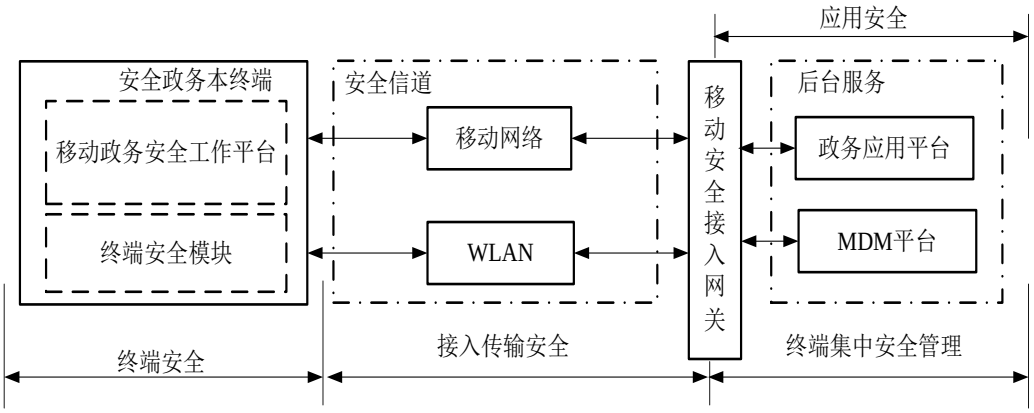

图 2 安全政务本整体安全框架

3.3 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：

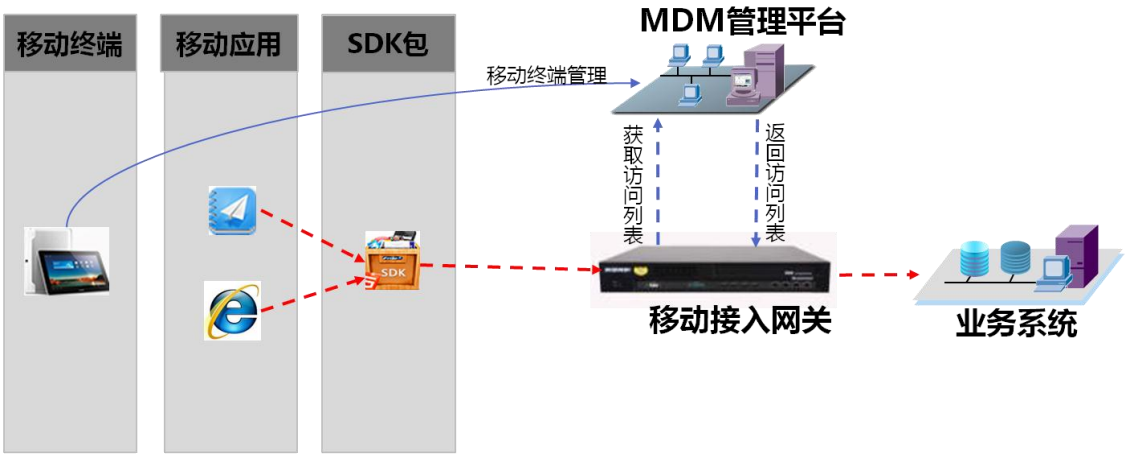

图 3 安全政务本安全接入逻辑架构

四、 服务管理平台(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。从长远应用考虑，在云平台上的移动终端管理系统(MDM)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，安全政务本系统将会适应这种类型的应用需求。云平台上的移动终端管理系统（MDM）的推广应用也是推广电子政务云应用很好的切入点。

安全政务本技术标准联盟根据实际需求构建“安全政务本服务管理平台”，其采用分级部署方式：国家核心管理平台和各省省级管理平台两个级别。国家核心管理平台负责监控各省级平台及国家核心管理平台安全政务本运行状态统计工作；各省省级管理平台负责具体管理各省行政权限下所属范围内政务本的安全管控工作。

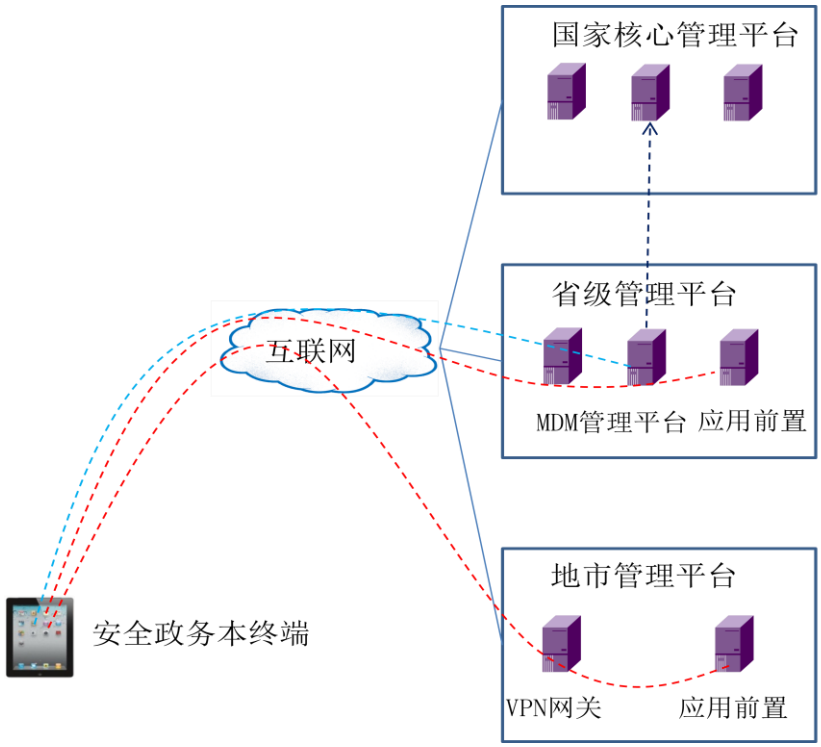

图 4 安全政务本服务管理平台全国架构体系

安全政务本管理平台以租用的模式服务于各级安全政务本使用单位。国家信息中心负责整个平台的运营维护，确保移动设备管理平台以及企业应用门户稳定有效，提供权限模板配置，为用户使用侧提供所需的权限模板。用户管理单位依靠权限模板所予权限，指导、管理、配置所管辖设备和应用，确保所辖用户设备安全、稳定、符合政务本使用安全标准，政务应用版本有效、可靠，符合设计预期，并向最终使用者提供有效服务。功能管理分配如下：

功能列表	用户管理侧	平台管理侧
用户管理	√	
设备管理	√	
策略管理	√	
安全合规管理	√	
报表管理	√	
应用门户管理	√	√

系统管理		√
日志管理		√

管理平台核心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。

图 5 MDM 管理平台核心功能

五、 测试与选型

5.1 测试规范编制

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》由安全政务本技术标准联盟组织国内信息安全专家和供应商编制。

5.2 产品测试

由安全政务本技术标准联盟与国内权威信息安全测评机构共同组织对该标准下的每套标准化系统进行产品测试，系统性能达到要求的才能获准使用安全政务本的名称。

5.3 应用系统安全测试

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，由安全政务本技术标准联盟和国内权威信息安全测评机构共同组织安全测试。

5.4 应用系统年检

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,可委托安全政务本技术标准联盟和国内权威信息安全测评机构进行系统的信息安全年检。

5.5 APP 应用测试

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会议制定,评测工作由国家信息中心信息与网络安全部和国内权威信息安全测评机构共同组织。

六、 与电子政务业务的融合

6.1 基本移动办公应用

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。

6.2 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，应用规模大，积累的经验多，其适应新应用的能力也会大大提高，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，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；

◆ 双因子认证：移动 APP 访问政务应用时，必须经过 CA 数字证书和登录密码进行双因子认证；

◆ 访问控制：移动 APP 支持基于时间属性的访问控制，可以配置允许用户登录业务系统的时间段，只有在允许的时间内，用户才能够登录访问内部网络的资源。

6.3 与云端数据管理的结合

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。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。

6.4 电子政务软件推送与下载

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。

6.5 应用领域

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。

七、 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由深圳市经信委组织，深圳市电子政务资源中心实施,福田等区县,经信委等委办局参与。其解决移动办公等移动化业务需求。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；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。

八、 选购方式

8.1 平板电脑供应商选择

目前安全政务本产品有如下五套版本：

华为版：华为平板 + 华为 MDM;

中兴版：中兴平板 + 中兴 MDM;

联想网秦版：联想平板 + 网秦 MDM;

壹本网秦版：壹人壹本平板 + 网秦 MDM;

壹本联通版：壹人壹本平板 + 联通 MDM;

8.2 通信运营商选择

可供选择的运营商有中国联通、中国电信和中国移动，其中联通公司完成了与华为版、中兴版的连接试点，联通公司将提供完整的终端配置、通信资源提供等服务。

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。

8.3 CA 运营机构的选择

安全政务本原则上对数字证书没有限制，只要是国家正式批准的具有电子政务服务资质的 CA 运营机构发放的证书均可使用。数字证书需要与安全政务本进行适配并完成规范测试。目前国家信息中心运营的“政务 CA”的数字证书已

完成了所需要的适配与测试工作，能够方便地适应全部五套系统，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。

8.4 支付方式选择

为方便各级政务部门的使用，安全政务本系统产品的支付有多种方式：

（1） 服务租赁模式。以租赁方式向用户提供终端、MDM、政务应用软件、安全、通信及运行维护等标准化服务。用户以租用的方式节省前期一次性投资的费用及后期的维护成本。

（2） 自建模式，用户自行购买终端、MDM、政务应用软件、安全、通信服务，运营商可以提供售前支持、售中实施、售后运维服务。

（3） 按年支付通信服务费，终端设备（PAD）由运营商提供；

三种支付方式由用户与供应商协商决定。

8.5 系统交付方式

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。

九、 机构与管理

9.1 领导机构与参与机构

安全政务本目的在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。安全政务本的标准化工作将在安全政务本技术标准联盟的领导下开展。

安全政务本的标准设计与其后的维护工作参与单位是：国家信息中心信息与网络安全部、中国软件评测中心、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、中国联通、中国电信、中国移动、网秦公司。

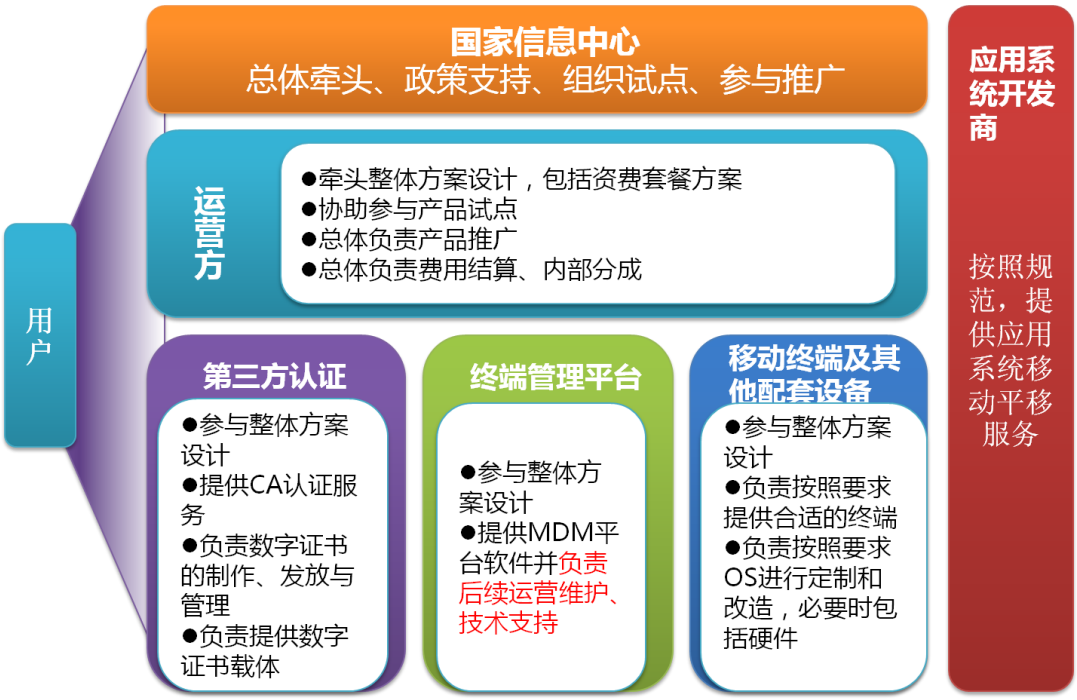

图 6 安全政务本成员架构

9.2 技术标准联盟

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。制定标准很重要，维护与推广标准更重要，安全政务本的标准维护与推广工作由安全政务本技术标准联盟来承担。联盟是非营利民间组织，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。

9.3 技术标准联盟办公室

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电子认证服务处，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。

9.4 品牌管理

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。

十、 引用与参考文件、术语定义、联系单位

10.1 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》

10.2 术语定义

（一）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。

（二） 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。

（三） 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 高容量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

10.3 联系单位

国家信息中心信息与网络安全部

地址：北京市西城区三里河路 58 号 100045

国家信息中心大楼 B 座 5 层

电话：010-68558503

联系人：国强