基于 SM2 的安全接入解决方案

一、 方案背景

随着 Internet 技术的不断发展，近几年国内企事业单位的信息化建设得到了快速发展，如网上办公、电子政务、电子商务等应用都得到了快速推进和发展。越来越多的政府、企事业单位已经依托互联网组建了自己的网上办公系统和业务应用系统，从而使内部办公人员、合作伙伴等通过网络可以迅速地获取信息，使得远程办公和移动办公模式得以实现。目前通过 Internet 进行安全接入和组网一般采用 IPSEC 或 SSL VPN 技术，通过 Internet 来组建了自己的私有网络，实现了企业总部与分支机构、合作伙伴以及移动用户的安全互联。

但随着密码技术和计算技术的发展，1024 位 RSA 公钥密码算法正面临日益严重的安全威胁，为保障重要经济系统密码应用的安全。国密局已于 2011 年 3 月下发了《关于做好公钥密码算法升级工作的通知》（国密局字[2011]50 号），对公钥密码算法升级的有关工作做出了具体安排。按通知的要求，自 2011 年 7 月 1 日起，新投入运行并使用公钥密码的信息系统，应使用 SM2 算法；已投入运行的，应尽快进行系统升级，并使用 SM2 算法。

因此，对于目前已经广泛应用的 VPN 安全网关系统，也提出了新的升级改造要求，需要能提供基于 SM2 的全新 VPN 解决方案。由于现阶段国内 VPN 产品使用的公钥密码算法主要是 RSA，新的解决方案要求使用 SM2 椭圆曲线算法来替换 RSA 公钥密码算法。

SM2 算法相比 RSA 算法具有如下优势：签名速度和密钥对生成速度都远快于 RSA；ECC 算法的单位安全强度高于 RSA 算法，也就是说，要达到同样的安全强度，ECC 算法所需的密钥长度远比 RSA 算法低；数据表明，ECC 256 位（SM2 采用的就是 ECC 256 位的一种）安全强度比 RSA2048 的还高，但运算速度要比 RSA2048 快的多。

二、 安全需求分析

根据政府、企事业单位等网络信息系统建设的需要，在实现总部与各级单位、分支机构网络安全互联及移动办公安全接入的同时，结合国家对相关网络通信协

议及加密算法的要求，其主要安全接入需求如下所述。

1. 应用系统的适应性与安全性需求

远程接入网络需要承载的业务系统种类较多，且对于应用系统的实时性和可靠性有较高要求；网络应用需要基于 B/S 和 C/S 架构，业务模式较复杂；远程接入移动办公人员众多，且需要能同时支持 PC、PAD、智能手机等多种终端接入。

2. 网络通信协议及加密算法的安全性需求

对网络数据及传输的安全性要求较高，数据加密的对称密码算法需使用国家密码管理局规定的 SM1 或 SM4 加密算法；摘要算法需要使用 SHA1 或 SM3 算法；用于证书认证的非对称密码算法需采用国家商密 SM2 算法，且 CA 系统需要支持国密局《SM2 数字证书规范》。

通信协议需要符合国密局制定的国家技术标准，即符合《SSL VPN 技术规范》和《IPSEC VPN 技术规范》

3. 设备与用户的管理与安全性需求

对所有网关设备和远程接入用户采用统一、严格的身份认证和集中管理；能实时监控设备及用户工作状态，并进行详细日志记录；整个远程接入系统安装方便、快捷，便于维护和管理。

三、 解决方案

根据政府、企事业单位分支机构网络互联及移动用户安全接入的实际需求，我们采用专门的 VPN 密码机产品提供基于 SM2 的 VPN 远程安全接入解决方案，解决其所面临的远程安全接入、传输保密、用户认证、网络安全防护、访问控制等问题，具体解决方案及网络拓扑结构图如下：

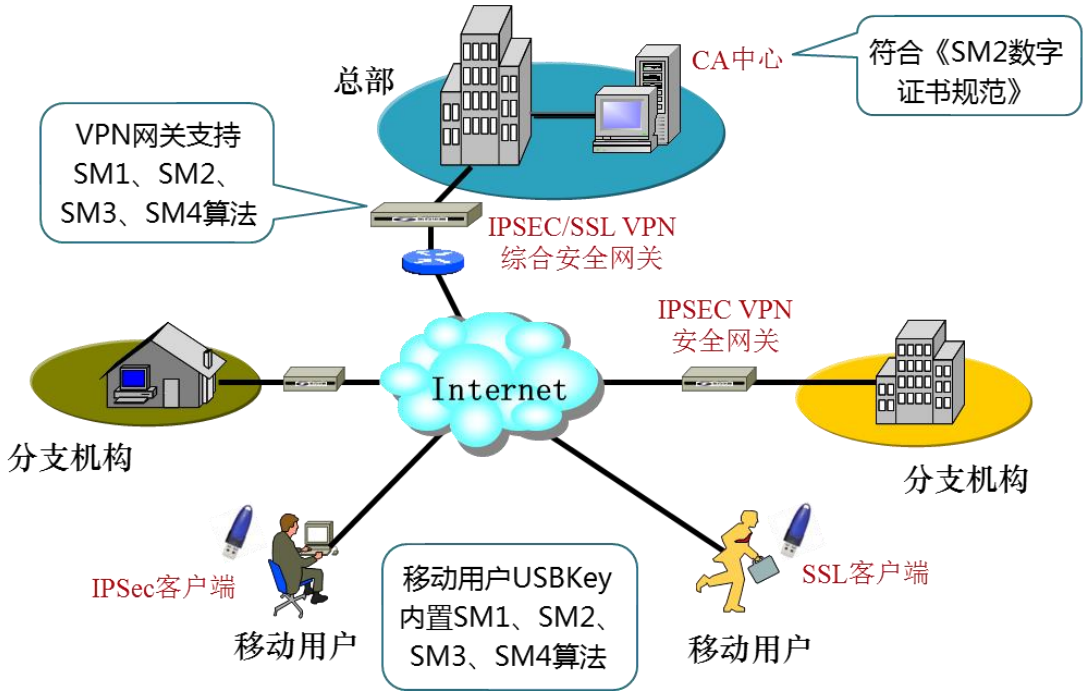
1、 在总部网络中心部署高端 IPSEC/SSL VPN 综合安全网关，作为中心 VPN 密码机安全接入网关。中心和分支 VPN 密码机都内置有硬件加密卡，支持 SM1、SM2、SM3、SM4 等国产加密算法，并符合国密局 VPN 技术规范。同时，通过 VPN 综合安全网关集成的防火墙功能可提供对内网的访问控制和网络安全防护。

2、 各分支机构根据网络规模部署相应 IPCEC VPN 安全网关，作为分支 VPN 密码机安全接入网关。分支网关在连入互联网的同时会自动向中心 VPN 安全网关进行身份认证和 VPN 隧道协商。同时，分支网关还可以提供

防火墙安全防护功能。

3、 在总部部署 CA 服务器，用于为所有 VPN 网关和移动用户颁发 SM2 算法的证书，采用证书方式对 VPN 设备和用户进行身份认证，且 CA 符合国密局《SM2 数字证书规范》。

4、 移动办公用户在终端上安装 IPSEC 或 SSL 客户端进行安全接入，采用在 USB Key 上写入的 SM2 证书进行身份认证，且 USB Key 自带加密芯片，支持 SM1、SM2、SM3、SM4 国产加密算法。



四、 应用案例

某省电子政务外网为实现各级政务部门之间业务系统的网络贯通，需要为部分不具备专线接入政务外网的政务部门以及一些偏远地区提供安全接入。另一方面，众多政务部门出差人员或移动办公的人员也需要能方便的接入业务系统进行数据上报。

根据此电子政务外网的安全接入需求，我们在省级中心部署了高端 SJJ1209 IPSEC/SSL VPN 综合安全网关，用于提供各级政务部门和移动办公人员安全接入，在各级政务部门部署相应中低端 SJJ1209 IPSEC/SSL VPN 综合安全网关接入省中心。同时，在省中心部署安全策略管理中心，便于对所有设备和用户进行集中监控、身份认证和通讯策略管理。另外，为保证通讯和数据传输的安全，VPN

安全网关及客户端全部使用了 SM1、SM2、SM3 国产加密算法和国密 VPN 协议进行身份认证、加密和数据传输。

通过采用基于 SM1、SM2 等国密算法的 VPN 安全接入解决方案，实现了某省电子政务外网业务网络系统的安全互联和移动办公用户的安全接入，达到了理想的应用效果。

五、 商用密码产品清单

SJJ1209 IPSec/SSL VPN 综合安全网关

SJJ1221 高速 VPN 安全网关

SJK0801-B 高性能 64 位 PCI 加密卡