企业网络中 3G 接入安全解决方案

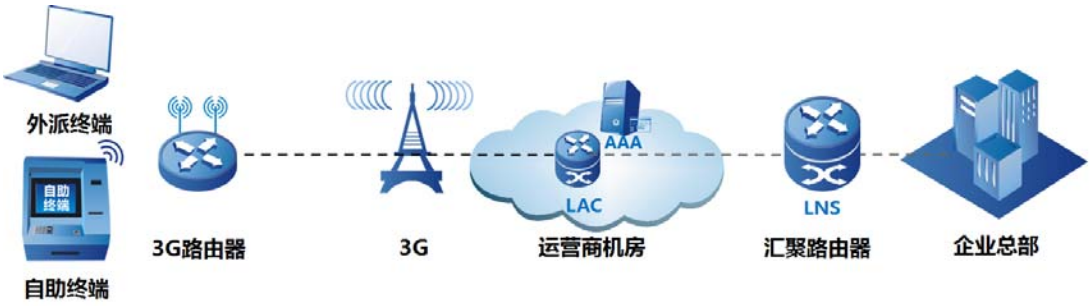
1　3G 联网的兴起

随着 3G 移动网络的迅速普及，各大运营商在提供更多基于 3G 多媒体业务的同时，也给个人用户及企业客户带来更高带宽的无线接入体验，3G 作为灵活、快速、安全、高效的广域网接入方式，已逐步成为用户广域网接入的新兴主流选择。

3G 网络相对于传统网络具有不可比拟的三大优势：快速灵活部署、低廉运营成本、具备快速恢复能力。目前已经有成熟的解决方案用于满足移动银行、城市移动监控、企业分支接入、电子政务网络接入以及商业移动办公等场合。

2　3G 联网的安全威胁与解决办法

2.1　普通的 3G 联网方案



方案中企业需要部署的设备如下：

- 业务终端：企业业务的处理终端；

- 3G 路由器：将业务终端与 3G 网络互联；
- LNS 汇聚路由器：汇聚 3G 路由器流量与企业内部核心业务系统互联。

2.2 用户身份安全

威胁：必须保证接入企业私有网络的 3G 终端是合法终端，防止非法 3G 终端接入企业私有网络盗取信息。

解决：

- SIM 卡安全：通过对 3G 用户的 SIM 卡信息（ IMSI“的国际移动用户识别码”）进行绑定，只允许绑定后的 SIM 用户通过用户名、密码认证后接入企业 3G 专用网络，防止非法 SIM 卡用户拨入企业 3G 专网进行非法活动。
- 3G 拔号安全：通过 3G 终端设置 SIM 卡的 PIN 码保护功能，只有知道 SIM 卡的 PIN 密码才能触发 3G 拨号，防止非法用户获取到企业 SIM 卡后进行的非法操作，保证了发起拔号的终端是合法用户在使用。
- 认证鉴权：通过 AAS/CMS 认证服务器能够对 3G 用户进行扩展认证，包含用户名、密码、IMSI 信息、终端硬件 ID 等多关键字的联合认证。

  在 CMS 证书管理服务器中需要使用公钥密码算法进行安全保证，通过采用经国家密码管理局批准的具有自主知识产权的 SM2 算法，增强了认证鉴权过程的安全性。

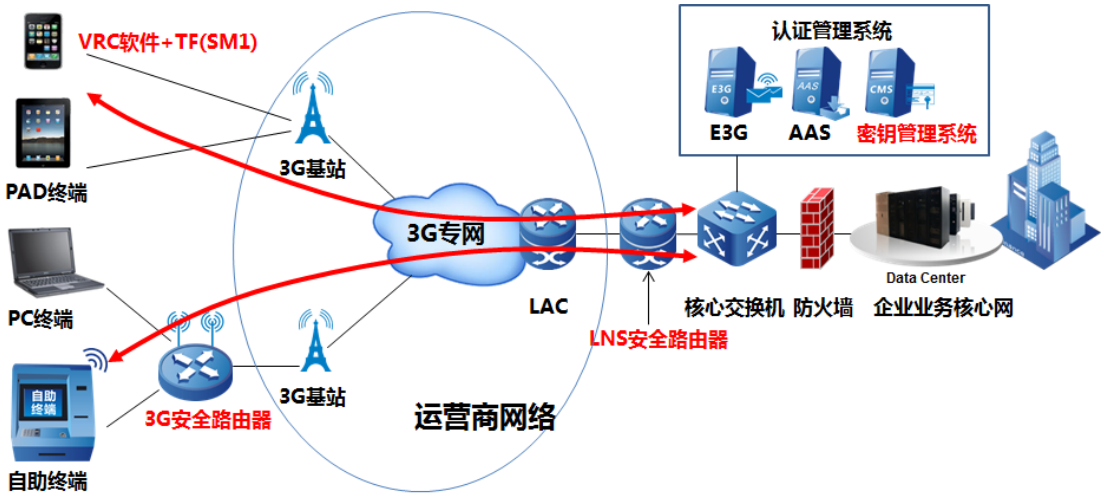
2.3 数据传输安全

威胁: 传统网络中使用的路由器主要提供网络接入、路由控制等，在安全性方面功能较弱，在利用 3G 数据网络传输 IP 数据包时通常未进行加密，若有非法用户在网络上探嗅到合法终端的正常通信数据包，就会造成数据传输的安全事故，这对 3G 接入场景下的 IP 数据包传输过程中的加密技术提出了新的要求。

解决: 设计一种安全路由器，将路由器的功能和必要的网络安全功能综合到一套系统中，并使用 SM1 加密算法对数据包进行加解密，为重要和关键行业系统提供一种安全、可靠、高效能的网络综合接入系统。

3 方案设计

3.1 总体方案



3.2 方案说明

企业网络中 3G 接入安全解决方案使用了如下关键组件:

- TF密码卡:实现SM1算法的TF卡安装于PAD终端,通过VRC(VPN Remote Client)以 IPSecVPN 协议并采用 SM1 加密算法安全地接入企业私有网络。
- 接入侧安全路由器: 3G 路由器与 LNS(L2TP Network Server)之间建立采用 SM1 算法加密的 IPSecVPN，实现安全接入企业私有网络。
- LNS 侧安全路由器: L2TP Network Server，接受 3G 终端的拨号连接，并与远端建立 IPSecVPN，实现远端的安全接入。
- 密钥管理系统: CMS，负责管理与颁发公钥数字证书实现 SM2 的证书管理，为 3G 终端的接入认证提供证书管理支持。

4 应用案例

4.1 省级卫生厅二、三级医疗信息共享平台

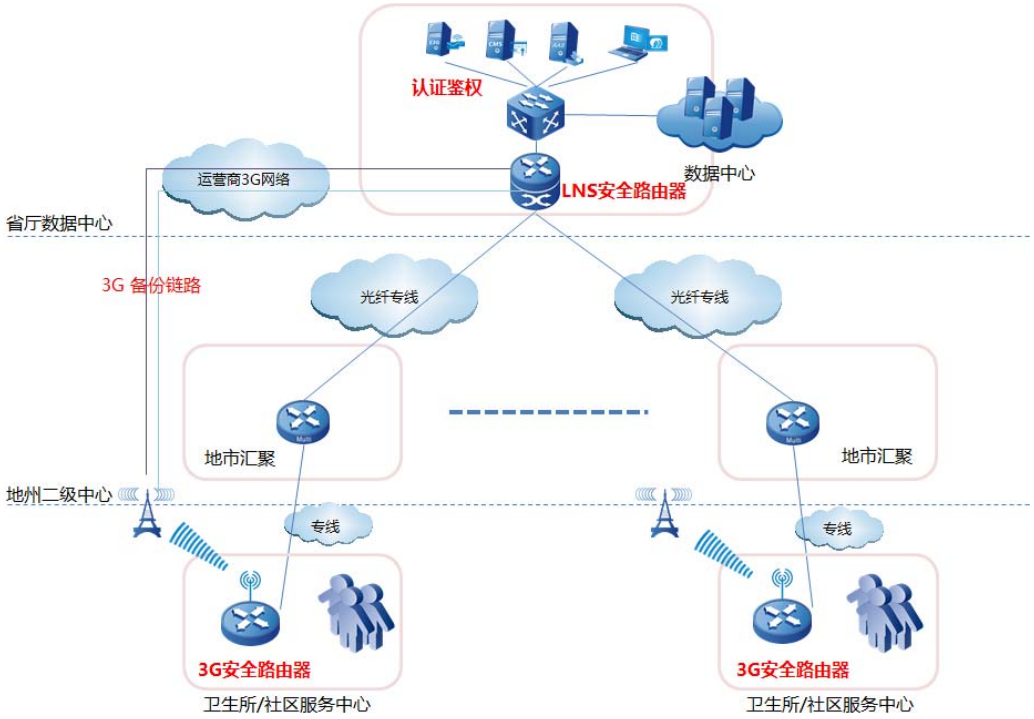
- **案例背景:**

国务院颁布的《关于深化医药卫生体制改革的意见》明确指出，务必把卫生信息化建设作为保障医药卫生体系有效规范运转的八项措施之一，建立实用共享的医药卫生信息系统，大力推进医药卫生信息化建设。

- **方案目标:**

在省卫生厅建设数据中心，各地市州建立二级中心，共享医疗卫生数据。

- **总体方案:**



➢ **实施效果:**

通过专线实现卫生所/社区服务中心与省厅数据中心的业务数据传输，当专线故障或所在地域无法铺设专线时，采用 3G 专网实现与省厅数据中心连接，使用 3G 链路时采用 SM1 加密算法对数据传输进行加密，保障基础网络架构能够满足卫生系统正常、稳定、安全、可靠运行。

4.2 银行离行 ATM 的 3G 接入

➢ **案例背景:**

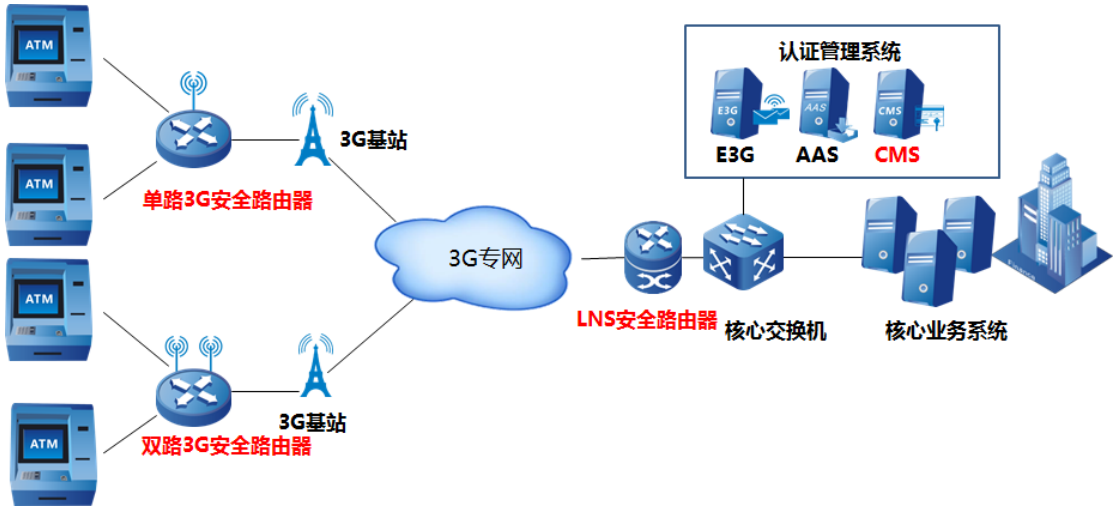
随着银行业业务竞争的加剧，上门服务和移动营销已成为各银行进行业务拓展和客户服务的重要手段。银行业务部门也提出了柜面业务延伸终端、离行自助服务终端的需求。在传统有线专线的环境下，对上述特色的移动业务无法实现快速有效的部署，同时进线受限的情况下网络高可靠性的支持也难以满足，迫切需要一种稳定性高、安全

性好、自由度高的接入方案解决上述问题，以便更好的为储户服务，满足移动接入/灵活接入业务的需求，需要进行离行 ATM 的部署。

- **方案目标:**

在全行范围内实现离行式 ATM(ATM 机部署在商业圈，住宅小区等地不依托于银行分支机构联网)，通过 3G 线路接入。

- **总体方案:**



- **实施效果:**

以安全、稳定、可靠的 3G 接入方式实现了银行各省分行的离行业务快速部署，实现了更大的网点覆盖率，服务满意度得到得升，增强了企业的竞争力。

5 商用密码产品清单

（1）加密路由器

（2）数字证书认证系统