密九云

基于国密算法的云安全接入解决方案

技术白皮书

OLYM® 奥联

OLYM 奥联

民族密码 奥联智造

深圳奥联信息安全技术有限公司

名词解释

IBC：IBC（Identity-BasedCryptograph）即基于标识的密码技术，是基于传统的 PKI(公开密钥基础设施)基础上发展而来，用户标识（如邮件地址）即是公钥，无需证书交互和验证过程，使安全应用易于部署和使用。

SM9：国家密码管理局关于标识密码的商用密码算法标准。

目　录

第一章　远程接入风险分析

1.1. 需求分析

随着信息网络技术的应用正日益普及和广泛，应用领域也从传统的、小型业务系统逐渐向大型、海量、关键业务系统扩展，所以鉴别使用人或设备的身份、保护使用者隐私信息、应用系统的安全性、数据的真实性和私密性等问题尤为重要。如何实现使信息系统不受恶意攻击和入侵，已成为各种应用系统信息化健康发展所必需考虑和解决的重要问题。

本方案主要是解决如下的应用场景：

1. 节点多、数据量大：上万客户端节点同时和中心点的安全通讯，包括语音和视频数据 ；
2. 传输通道要有安全保证：数据的传输必须经过加密防止泄露，设备接入必须经过身份认证，传输的数据不能被篡改；
3. 终端设备平台多样：支持各种终端节点设备，操作系统多样，硬件平台多样；
4. 不能影响用户的网络拓扑或 IP 设置：不能因项目的部署影响到用户的网络拓扑和 IP 地址设置。

1.2. 传统接入技术分析

解决安全接入，主要使用了如下一些技术，现分析如下：

方式一：IPSec VPN 技术

- 优点：可实现 LAN 到 LAN 的透明通讯
- 缺点：由于透明通讯，所以无法防止病毒木马传播，难以实现对应用和主机分离保护，比如 Windows 的 BadTunnel 漏洞充分暴露了 IPSec VPN 技术的安全性弱点；部署时候需要规划内网 IP 和外观 IP 地址，整体部署时候所有的网络地址不能冲突，这在节点众多时候很难实施；

方式二：SSL VPN 技术

- 优点：在应用层实现安全通讯，无需更改用户网络地址；

- 缺点：只支持 WEB 应用；如果要实现三层、四层应用需要安装控件，只能在 windows 系统上运行，如客户端设备是 Linux 则难以部署；

其他技术

其他如 PPTP、L2TP、GRE/IPIP 都存在各种不足。如 PPTP 安全性不够，也无法支持大容量的用户接入；GRE/IPIP 通道没有加密功能；这些协议在现在的市场情况也是日渐减少。

第二章　技术方案

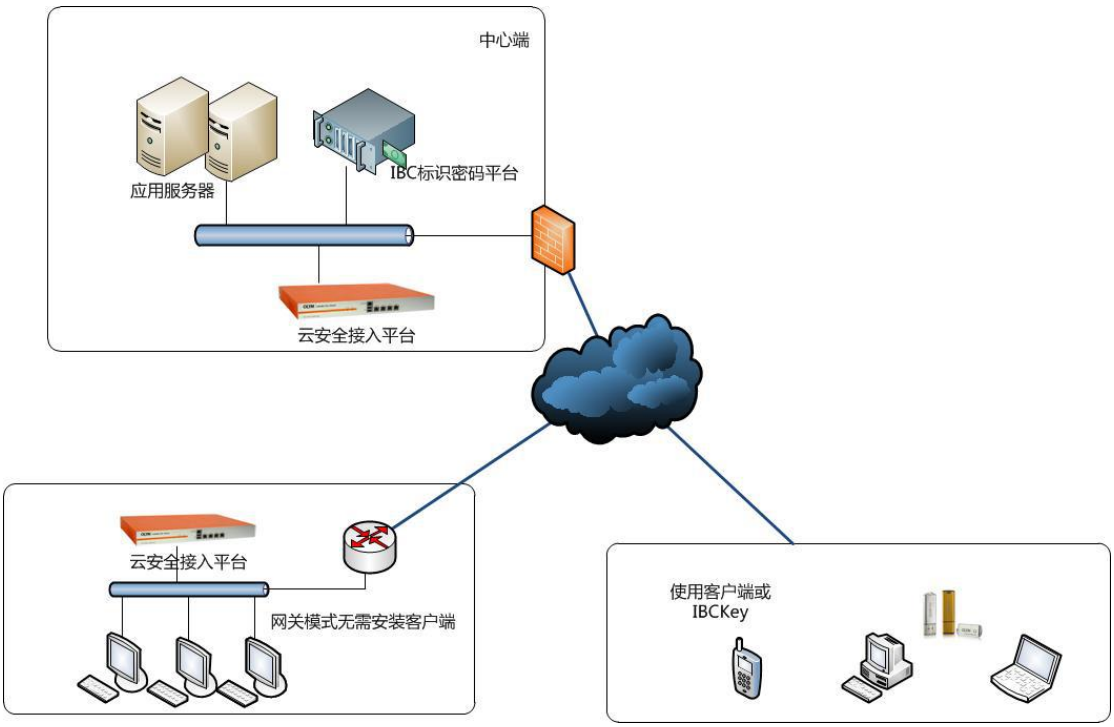
密九联是基于多种密码算法对移动智能终端和专用 PC 端访问服务端应用系统，实现强身份认证和通道加密功能，防止因系统漏洞、弱口令等造成应用系统冒名越权访问、数据篡改和数据泄露，保障应用系统的安全稳定运行。

2.1. 系统架构

密九联分为两个部分：

- 云安全接入平台：提供客户端接入功能，可单臂部署和网关方式部署。
- IBC 平台：用于 IBC 私钥的申请、产生和下发。如使用其他认证方式（如传统证书认证或用户密码认证等）则无需部署此平台。

系统具体网络拓扑如下：



图中客户端可选择安装专用客户端、IBCKey 或者部署硬件网关。

2.2. 技术路线

密九联安全接入采用 NTLS 技术来实现。NTLS，英文全称是 Next Transport Layer Security，它是我公司研发的传输层安全协议，采用多框架密钥交换协议和支持包括标识密码算法在内的各种国密算法，同时结合网络封包截获和代

理技术，实现远程访问用户的身份认证和远程数据的加密传输，让访问者更安全地远程访问远程内部资源。NTLS 通过简单易用的方法实现信息远程连通，并且采用密码技术对远程节点身份做强制认证，有效保证了远程访问和远程数据传输的可鉴别性和安全性。NTLS 安全通道方案可同时支持三、四层安全机制，三层安全机制可以实现站-站、站-网、网-网的数据安全保护，并对三层数据按照四层的安全策略进行控制。细粒度的安全策略可以保证系统免于传统 IPSec VPN 面临的安全风险。四层安全机制采用数据重定向技术，节点无需分配 IP，中心端无需开放某个 IP 或者网段给远端，支持基于端口、协议等多种访问控制和完善的访问日志记录，具有更高的安全性和可管理性。

另外，本方案支持标识密码技术(Identity-Based Cryptography：IBC)来实现身份鉴别。在基于标识的密码系统中，每个实体具有一个标识。该标识可以是任何有意义的字符串。但和传统公钥系统最大的不同是，在基于标识的系统中，实体的标识本身就用作实体的公开密钥，这样系统就不再依赖证书和证书管理系统，从而极大地简化了密码管理系统的复杂性。在具体应用系统中，用户可直接使唯一标识（例如身份证号、社保号、手机号、电子邮件地址）作为公钥，无需预先协商密码或者交换证书。系统的易用性和安全性得到完美的结合。

2.3. 实现原理

为更好了解方案，对以上方案中实现的原理进行描述：

2.3.1. C/S 模式安全通道实现过程

安全通道的建立主要通过客户端和服务器端来构成专用隧道。构成和形式如下：

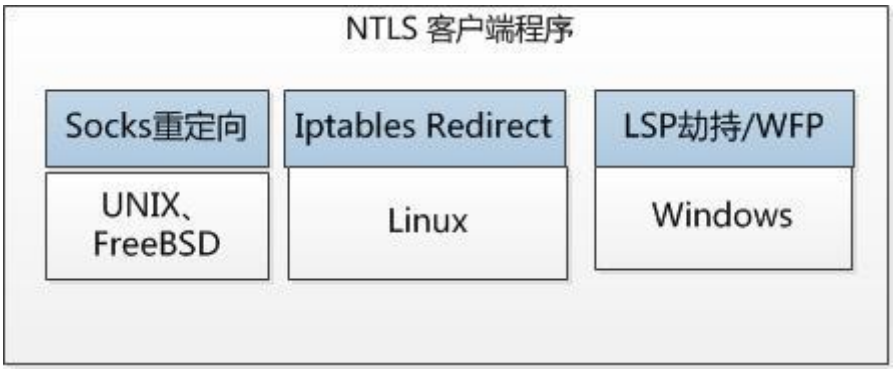
- NTLS 客户端：软件形式。可支持 Windows、Linux、Unix、iOS、Android 平台，基于标识进行身份认证，连接服务器端进行安全通讯；
- NTLS 服务器端：有软件形式和硬件形式两种。

  其中，软件方式可支持 Windows、Linux、Unix、iOS、Android 平台，仅提供接入功能；

  硬件形式为专用硬件设备：云安全接入平台，具备完整的用户管理、策略管理、日志管理、网络设置、资源查看等等功能。

通讯时，需要 NTLS 客户端向 NTLS 服务器端发起请求并建立安全通道，访问服务器端的资源。

NTLS 客户端到服务器端通讯的工作原理如下：



1、拦截特定的协议和端口、目的 IP：NTLS 客户端软件在不同的操作系统的不同采用了不同的数据拦截和重定向技术，以确保不影响原来的应用。基于 Linux 采用了 IPTables，基于 Windows 采用了 LSP 拦截或 WFP，均为系统内置，所以均无需对系统做任何调整；对于 UNIX/FBD 系统，只需预加载我们提供的一个库文件即可。

2、将其发出的相关数据进行加密，重新定向送到指定的 NTLS 服务器端；

3、NTLS 服务器端解密后还原其数据请求，并通过服务器指定的路由发出。返回的数据也是如此。

此设计不同于市场上普通的任何 IPSec 或 SSL 产品，基于应用层，无需改变用户的网络环境，而且对各种应用透明，具有安全和易于部署的优势。

2.3.2. 对等模式安全通道实现过程

对等模式下通道两端设备可以相互同时访问对方数据或应用。可以采用星型或网状部署。星型模式下由各个远端节点设备连接到中心点接入设备，具有安全策略统一管理的优势。中心点设备统一实现安全策略分发、虚拟 IP 地址分配、路由管理、IP 地址和域名映射等。远端节点设备连接到中心点接入设备后获取对应标识的虚拟 IP 地址和根据安全策略可以访问的路由。三层 IP 数据根据路由配置进入安全通道。安全通道根据获取的安全策略进行策略匹配，不符合的策略数据将被抛弃。中心点设备在收到远端通道发来的数据后再次进行策略匹配，不符合的策略数据将被抛弃。合法数据会进一步路由到目的地，目的地可以网络内设备或者是其他安全通道后的远端网络。

2.4. 海量用户接入说明

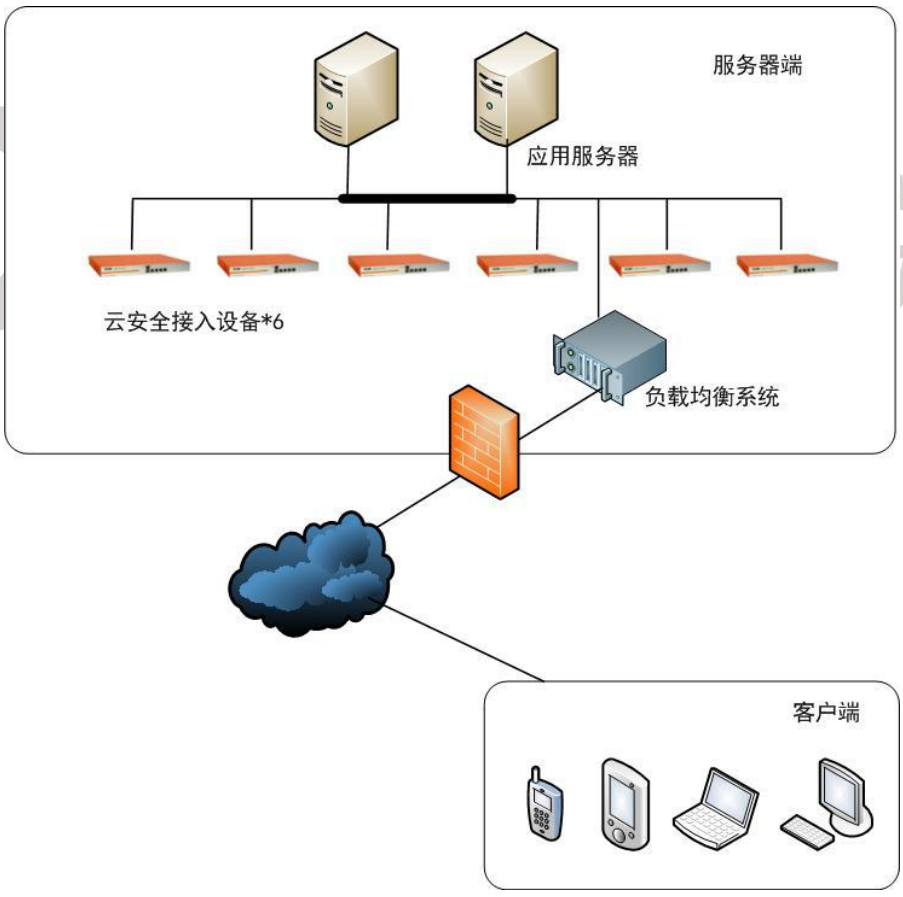
本方案涉及的核心产品的性能可满足以下指标：

2.4.1. 单台云安全接入平台性能描述

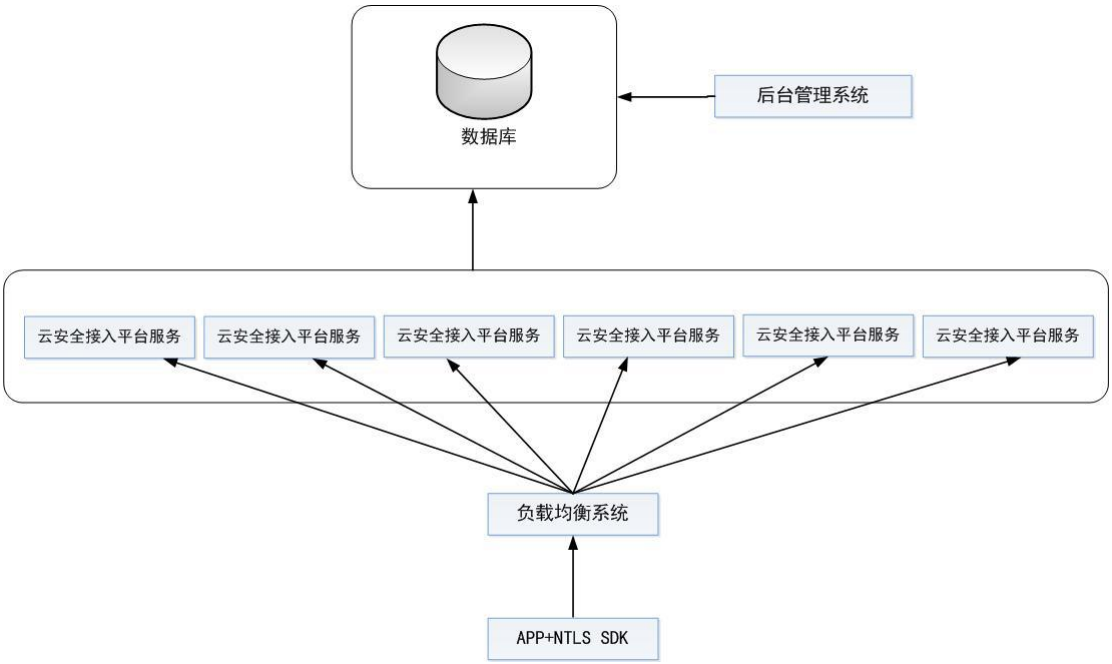
- 主要性能指标：加密速度不低于 800Mbps、应用会话数可达 64K、隧道并发数可达 16K。
- 可通过级联、负载均衡达到海量接入。

2.4.2. 海量用户部署说明

如按单台用户支持 5 万用户设计，海量用户部署拓扑图如下：



其实现原来是利用负载均衡系统实现负载均担，并通过分布式数据库实现多台接入服务设备同享统一数据库。原理图如下：



2.4.3. 客户端性能描述

客户端性能主要取决与其硬件平台的性能。由于每个客户端只负责建立一条通道，所以目前客户端的硬件（PC 或智能手机）都可以胜任。

2.5. 加密算法扩展

方案中使用的加密算法均可扩展：

- 对称算法：用于保障通道中的数据加密，可扩展用户自定义算法；
- 非对称算法：用于身份鉴别和签名运算，也可以扩展用户自定义算法。

第三章　部署方式

3.1. 用户端（C 端）部署方式

3.1.1. 硬件 KEY 方式

由于大多数客户端都是 Windows 系统，所以可采用我公司的内置安全接入客户端的 IBCKEY 硬件接入方式。

IBCKey 内有专用的密码保护芯片，并通过国家密码管理局的技术鉴定，支持 RSA、标识密码算法 SM9、SM1、SM2、SM4 等各种算法。自带安全存储区（存储 IBC 私钥或 PKI 证书）、falsh 区（内置安全接入客户端）。

插入 KEY 后客户端自动运行，用户无需设置。使用效果如下：

3.1.2. 软客户端方式

对于不想携带硬件 KEY 方式的用户，可以登录云安全接入平台页面直接生成自己的专用客户端软件。

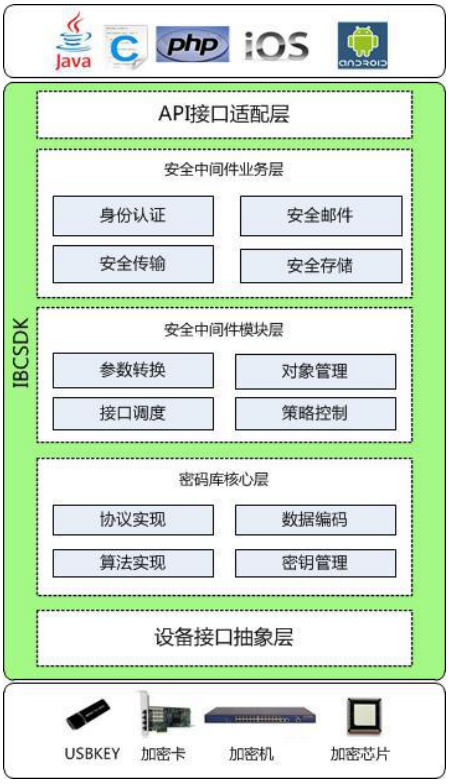
软件客户端使用了文件私钥，这是通过口令方式保护用户私钥信息，并以文件方式存储在电脑或智能终端里。文件私钥具备部署成本低、使用方便的优点。

软件客户端也可以简化为一个服务程序，启动后自动运行，自动完整认证。

3.1.3. APP+SDK 方式

可提供客户端开发的 SDK 接口，用户 APP 通过几个函数调用即可实现安全接入到云端。此方式无需改变用户的使用习惯下即可实现实现安全连接。

SDK 可支持 Andorid、iOS、Linux、Macos 系统，通过我们提供的范例源代码，可在极短的时间内完成开发。通过调用函数建立连接后，应用程序无须改动即可访问远端的内网资源。



SDK 已经为各类开发语言提供了可访问接口及示例，目前主要有：object-c，C/C++，C#，DELPHI，JAVA，PASCAL，PHP，脚本(com 组件)等，其它的语言可以使用提供的 CLI 来扩展使用。

经过以上参数配置（大部分默认，只需 IP 和端口），即可实现 APP 的透明访问。

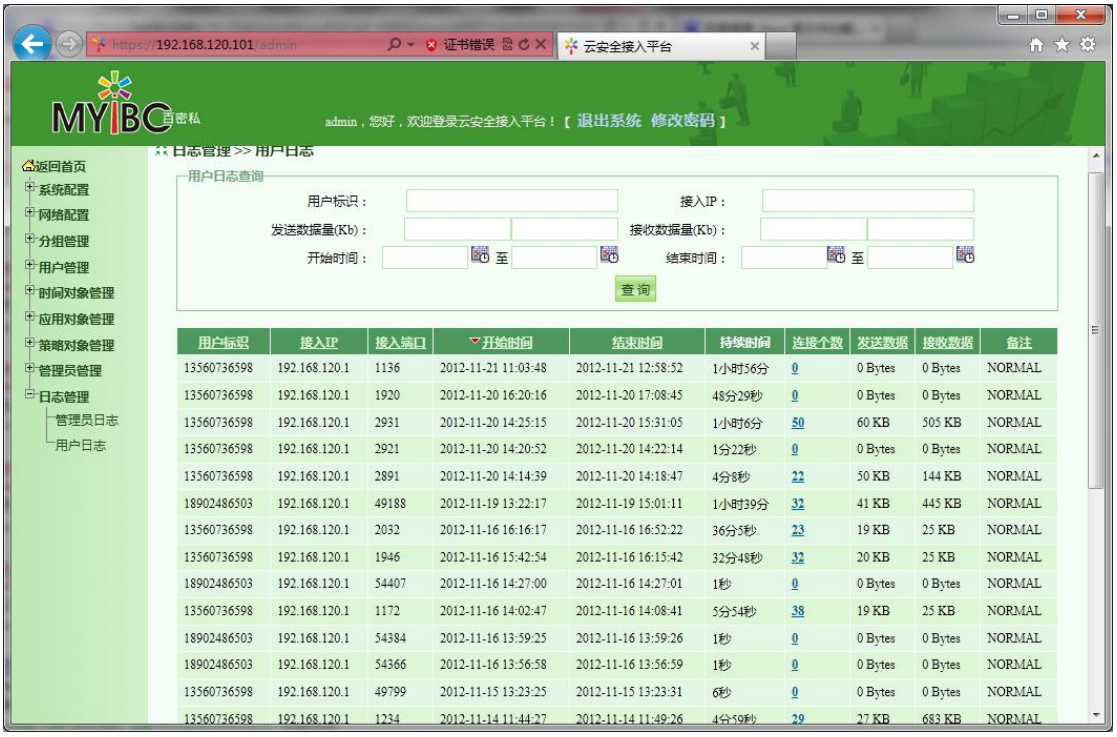
3.2. 中心端（S 端）接入设备部署说明

中心端接入设备直接部署云安全接入平台即可。

云安全接入设备根据可支持用户数有多个型号供选择。可以单臂模式、网关模式部署。**也支持云模式部署（无需硬件）。**

此方式实现了安全透明传输，无需对现在应用系统进行任何调整和改造。部署后接入需要通过云安全平台认证之后，才能使用原来的应用系统，数据的传输经过加密算法保障。云安全接入平台可根据客户端接入的标识、时间、可访问的应用、端口来设置各种安全策略：

部署后，只有通过云安全接入平台认证通过的用户才能访问访问应用服务器并会形成详细的访问日志：



另外，在特定应用场合下也可将接入服务器模块嵌入到中心端现有系统中。如嵌入到网络摄像头、现有应用服务器等。但此模式只提供接入功能。

3.3. 远端（P 端）接入设备部署说明

在对等模式下部署云安全接入设备，配置其和中心端云安全接入设备进行连接。如果要在远端设备上支持移动用户接入，可以采用中心端设备类似的配置。

第四章　方案优势

本方案具备以下优势：

1) **支持各种国密算法**：系统模式支持国密和国际标准算法，包括：SM9、SM2、SM3、SM4、SM1、RSA、AES、SHA1、SHA2、SHA3、ECSRP5、HMAC、DEM 等算法。可以方便扩展支持专用算法。
2) **高安全性性**：使用非对称算法进行双向身份认证，使用对称算法对数据加密和一致性保护。每个链接的会话密钥动态协商，保证每个客户端到服务器之间通讯的会话密钥都不一样，实现了高强度的安全保障；无需担心 SSL 协议、开源代码中的协议实现漏洞等问题。
3) **基于应用层的策略控制**：基于应用层策略实现了安全传输控制，所有操作均可控，不同于普通 IPsec 或 SSL，可杜绝病毒通过通道传播；
4) **详细的日志记录**：在云安全接入平台上，可以记录每一个标识访问的详细日志；基于应用的访问控制，如限制每个用户只能进行某一项操作，访问指定的 IP 或者端口；并能形成详细的日志；
5) **支持两种组网模式**：完美支持移动接入等 C/S 模式，同时支持对端组网模式；
6) **不改变网络结构**：四层安全机制无需分配虚拟 IP，无需调整系统防火墙策略，即可实现安全通讯；实现了数据的透明传输，对现在的网络结构没有任何影响。
7) **高性能**：基于应用层的设计，不触及操作系统内核、不涉及驱动底层，可实现高性能数据传输、海量用户并发接入；
8) **支持 IP 地址管理**：内置虚拟 IP 地址分配、映射、转换等功能。支持在 ID 和虚拟 IP 之间进行转换，通过 ID 到域名到虚拟 IP 的管理实现便捷地终端设备标识、管理、访问。
9) **应用透明**：通过客户端到服务器端的安全链接，客户端可直接访问服务器端资源，原有应用无需二次开发。
10) **支持各类终端系统**：客户端支持包括 WINDOWS、LINUX、iOS、Android 以及各类嵌入式设备。

和普通的安全接入方案相比，本解决方案具有以下特点：

比较项目	NTLS	SSL	IPSec
用户端部署模式	软件模式和硬件设备均可。不改变客户网络任何设置 ★★★★★	客户端部署只能是windows系统，也支持IE浏览器，适用面很窄 ★☆☆☆☆	使用硬件设备，易于使用。但需要用户分配IP地址；如果上万节点的时候，中心点的网络规划会有较大影响 ★★★
用户端身份鉴别	可基于设备ID、用户单位名称、或其他自定义唯一标识来鉴别，通过SM9算法保障身份安全 ★★★★★	基于用户名或者证书。用户名不安全，证书则需要为每个设备申请和颁发设备证书，管理和配置比较繁琐。 ★★★★	由于是透明通讯，只能通过IP鉴别，无论是管理和操作在大用户量的情况下会非常麻烦。 ★★
使用方式	直接访问应用，如同在内网使用。所有应用内置，即插即用 ★★★★★	先登录SSL门户页面，通过认证后，再选择需要应用，跳转到应用页面 ★★★☆☆	透明模式，通过IP访问。 ★★★★★
使用日志	可记录每个客户端访问的详细日志。来源IP、目的IP、端口、协议等。 ★★★★★	可记录客户端详细日志。但鉴于可运行的客户端极少，参考意义不大。 ★★★	透明访问，记录IP包的加解密日志没有任何意义。 ★★
安全性	双向认证，更安全 ★★★★★	单向认证 ★★☆☆☆	通讯安全有保障。应用安全需配合其他措施（如防毒软件）

			★★★
移动智能设备	支持android系统、ios系统，和浏览器无关 ★★★★★	需要浏览器而定 ★★★☆☆	试产品而定 ★★★★
适应性	透明访问，几乎无限制 ★★★★★	一般B/S支持IE和chrome等主流，一旦需要控件方式，只能支持IE ★★★☆☆	透明访问，几乎无限制 ★★★★★
访问策略	可以基于端口、协议在应用层设置访问策略，病毒和木马不会通过通道传播 ★★★★★	可以基于端口、协议在应用层设置访问策略，病毒和木马不会通过通道传播 ★★★★★	可以基于端口、协议在网络层设置访问策略，病毒和木马可能通过通道传播 ★★★★
集中管理	可以集中配置和管理，策略通过中心下发 ★★★★★	可以集中配置和管理 ★★★★★	由于是对等传输，所以必须是两边同时配置。当到达一定数量之后，几乎是难以管理。 ★★

第五章　典型应用场景

5.1. 某省计生云安全接入应用

该项目是于中国电信某省公司合作，通过部署安全接入平台使某省省计生人口系统成功覆盖到全省所有地、市的计生部门和医院，实现了全省 60,000 多个乡村的人口、健康信息安全、快速汇总到省计生系统中。这样大量的用户部署如使用传统技术手段将十分繁琐，而使用 IBC 身份认证和云安全接入平台，用户只需输入自己的手机号码并将收到的验证码填入，平台即可生成该用户专享绿色客户端，下载后立即使用，无需其他设置，非常适合海量用户的快速部署。通过开放的 SDK 和 SOAP 接口，与用户现有应用系统实现单点登录，直接打开应用系统。

该案例充分体现了密九通安全接入方案对海量客户端接入支持优越性：方便地支持大量用户的管理、身份认证、安全接入。用户使用手机号码为标识方便结合电信计费，使用 SM9 标识密码算法和手机标识密钥对用户和业务系统进行双向身份认证，无需证书分发，节约费用，方便易用、安全性高。单机同时支持 6 万用户在线，系统效率高。

5.2. 视频安全应用

该项目用于某单位工作人员在全国各地以及世界各地的分支机构进行网络视频会议时对数据进行安全保障。各地人员使用标准的视频会议设备，通过卫星网络进行联线。因网络组成的特殊性，网络延时平均在 500ms。密九联安全接入方案因其采用的安全机制和实现方法不仅保障了其通道支持特殊安全性需求包括算法定制等，还能够在高延时的网络环境下支持 720p、1080p 等高清视频会议。

该案例充分体现了系统的高安全性，满足了特殊的极高安全性需求，同时也体现了在特殊网络环境下的良好适用性和高效率。

5.3. 物联网安全应用

伴随着物联网的兴起，物联网的安全性问题也日益突出。密九联安全接入方案在物联网中也有广泛的应用场景。在工业控制领域，远程传输终端是个典型的支持远程数据采集、指令执行的工业控制设备。在数据采集、指令传递过程中设备接入以及管理员人员的身份认证、数据的保密性以及完整性都非常重要。密九

联安全接入方案的安全客户端支持各类嵌入式设备，包括如 MIPS、ARM、X86 等芯片设备。将安全客户端嵌入到工业控制设备后，使用设备的编号作为标识生成标识密钥就可以实现和中心点接入设备的安全接入。中心设备后的控制服务设备就可以和设备进行安全通信实现数据采集、指令下达等。管理人员使用 USB Key 远程连接到中心点接入设备后，可以使用设备 ID 作为主机名查询到需要管理的远端设备 IP 进行远程管理，无需再为 IP 地址变化烦恼。中心点接入设备使用管理员 ID 和设备 ID 进行策略配置，控制管理员人员可以管理的设备组。另外在智能家居领域，将安全客户端嵌入到智能家居设备如家用网络摄像头、家庭智能控制终端等，就可以使用手机上的安全 APP 对家庭中的智能设备进行安全访问。安全 APP 可以使用用户的手机号码作为标识生成标识密钥。智能设备和安全 APP 之间通过执行高安全的身份认证和密钥协商协议后通道数据被全程加密保护。用户无需担心隐私泄露。另外如果需要将设备访问权限分享给亲朋好友，只需将好友的手机号码加入到设备允许访问的标识列表即可，无需转发口令等秘密信息，安全易用。

第六章　扩展应用

6.1SM9 算法简介

为了降低公开密钥系统中密钥和证书管理的复杂性，以色列科学家、RSA 算法发明人之一 Shamir 在 1984 年提出了 IBC 的设计理念。IBC 是 Identity-Based Cryptography 的简写，意为“基于标识的加密技术”，即用户的标识就可以用做用户的公钥（更加准确地说是用户的公钥可以从用户的标识和算法指定的一个方法计算得出）。在这种情况下，用户不需要申请和交换证书，从而大大降低系统的复杂性。用户的私钥由系统中的一个受信任的第三方（密钥生成中心）通过标识私钥生成算法使用主密钥和用户标识计算得出。这样的系统具有天然的密码委托功能，也非常适合于有监管的应用环境。

标识密码（IBC）技术作为近 10 年来密码学领域的重要突破，因其扎实的理论基础、良好的可用性，快速从理论研究进入到市场化、产业化、标准化阶段。

从国外发展现状来看，基于标识的密码技术在商业应用（特别是在欧洲和北美地区）中取得了巨大的进步。IBC 标识密码技术能够从一个重要的学术研究成果快速转变为成功的商业化应用主要得益于标识密码系统的简单性。最终用户的总体拥有成本相较于传统的证书机制有显著的降低。如 HP Voltage、SendMail、Proofpoint 以及台湾趋势科技等厂家纷纷推出了基于标识加密技术的邮件安全产品，在欧美市场的银行、零售、保险、能源、医疗保健等行业和政府系统得到广泛应用和部署。此外 IBC 标识密码技术还广泛应用在物联网、智能终端安全、云存储安全等应用中。

我国政府也非常重视 IBC 标识密码技术的推广应用。2006-2007 年，国家密码局组织了国家标识密码体系 IBC 标准规范的编写和评审工作。奥联作为标识密码算法的主要发起人，参与了多项标准制定工作。经过近 10 年的实践论证，2016 年 3 月国家密码管理局正式公布了中国的标识密码算法：SM9 算法。

SM9 算法是一种区别于传统公钥算法的标识密码算法。基于该算法的密码系统可使用具有唯一性的各类标识作为公钥，即可以使用如：邮件地址、手机号、身份证号、组织机构代码、物联网设备标识等作为用户或设备的公钥，进行数据加密和身份认证。SM9 因其算法特点，非常适合电子邮件保护、公文安全流转、多媒体融合安全通讯、身份认证、物联网安全通讯、云数据保护等应用。基于

SM9 算法的密码系统可方便地进行集中管控，实现方式简洁、成本低廉、应用场景广泛，具备快速推广的条件。

SM9 算法采用椭圆曲线上的双线性对作为基础数学工具，基于相关的计算复杂性假设构建安全性证明。其算法的理论基础、算法构造都经受住了安全考验。我国也正在积极推动将 SM9 算法纳入相应国际标准。

经过十年发展， SM9 算法在电子政务安全、移动终端安全、工业控制安全、物联网连接安全、税务票据安全、个人隐私保护等诸多领域已经有了众多应用。相关密码系统充分体现了算法的易于使用、便于管理的特色，为应用系统的安全运行发挥了重要作用。伴随着算法对社会正式公开，可以预见将有更多的应用系统将会采用该算法进行安全防护，进而提高我国信息安全的防护水平。

6.2IBC 系列产品

我公司致力于 IBC 技术的开放和应用推广，已经推出 IBC 标识密码平台、加密短信、加密邮件、加密文件柜、远程安全接入、IBC 安全中间件全线产品，可为用户提供全方位的 IBC 标识密码技术解决方案。

IBC 整体安全解决方案，通过邮件地址或手机号等作为身份标识，实现如下功能：

- 身份认证：用 IBCKEY 替代用户名密码登录，保证信息安全性；
- 数字签名：保证数据不被篡改；

- 数据加密：对数据进行加密，加强 OA、财务系统安全性；
- 安全接入：通过 IBCKEY 实现远程办公，随时随地接入内网；
- 邮件加密：对邮件进行加密收发，保证信息传递安全；
- 加密存储：对本机文件或 U 盘文件进行加密，有 KEY 才能解密；
- 短信加密：手机短信加密收发；
- 其他应用：IBCKEY 可结合奥联 IPSecVPN 产品、上网行为管理产品，实现远程登录和身份鉴别。