
密九盘

基于国密算法的加密云盘安全解决方案

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

目 录

1. 前言.....	2
2. 密九盘简介.....	2
2.1. 私有云模式.....	2
2.2. 公有云模式.....	3
3. 密九盘的系统组成.....	3
3.1. 私有云模式.....	3
3.1.1. WEB 前端业务系统.....	3
3.1.2. WEB 后台管理系统.....	6
3.2. 公有云模式.....	9
3.2.1. 登陆认证模块.....	10
3.2.2. 上传文件加密模块.....	10
3.2.3. 下载文件解密模块.....	10
3.2.4. SM9 密码机.....	10
4. 密九盘的功能.....	10
4.1. 私有云模式.....	10
4.1.1. 后台管理功能.....	10
4.1.2. 文件安全管理功能.....	12
4.1.3. 文件安全分享功能.....	13
4.2. 公有云模式.....	14
4.2.1. 云盘文件加密.....	15
4.2.2. 云盘文件解密.....	15
4.2.3. 无缝对接第三方云平台.....	16
5. 部署方式.....	16
5.1. 公有云系统部署方式.....	16
5.1.1. 桥接模式.....	16
5.1.2. 路由模式.....	17
6. 密九盘的特点.....	17
6.1. 基于 SM9 的国密算法.....	17
6.2. 文件安全管理、存储加密.....	18
6.3. 文件安全分享、灵活方便.....	18
6.4. 云端密钥管理.....	19

1. 前言

随着企业信息化建设的日益深化，企业大量的信息采用电子文档的形式进行存储、使用和交流。信息电子化为企业在文档的存储、使用、交流带来巨大的便利的同时，也带来了多种安全问题，如：

- 其他人能够在不经过允许的情况下能够通过网络窃听的方式监视企业在互联网上传输的电子文档信息；
- 企业员工出差在外，使用宾馆或者公共场所的网络访问企业的电子文档服务时，很可能在不知情的情况下泄漏了企业的机密信息；
- 电子文档被我们期望的接收者查看之前，可能会被其他人恶意的修改；
- 电子文档在上传和下载传输过程中或者本地存储后，被病毒、木马或别有用心的人窃取；
- 企业的文件服务器上的重要数据，会被 IT 的运维人员窥视这些重要文档的内容，造成敏感信息泄露；

企业机密信息大多以电子信息方式存在，而电子信息是很容易传播。目前大量的信息泄密往往是内部泄漏出去，防火墙、入侵检测等防护系统起不到任何保护作用。防火墙或专网只是解决了外部人员非法访问的问题，不能解决内部人员通过电子邮件、移动硬盘或笔记本电脑把电子信息进行非法传播的问题，也不能解决电子文档在网络传输过程中的泄密问题。

根据企业用户业务形态、办公流程、信息机密等级等需求来看，企业用户对电子文档存储和分发的安全要求如下：

用户身份的强鉴定：基于公私钥密码技术的身份认证机制，再结合手机短信码和登录设备绑定等双因子认证方式，强制有效的认证系统用户或者管理员的身份，防止用户身份被轻易伪装。

数据传输的安全性：在电子文档上传或下载的网络传输过程中，对数据传输通道进行加密保护，防止数据在传输过程中被窃听；

数据访问的安全性：采用访问控制技术并结合加密技术，只有指定的文档查看人才能访问到数据并查看内容，防止数据被未授权的第三方获取；

数据存储的安全性：电子文档数据都是以密文的形式存储在服务器上，即使未授权的第三方能获取到数据本身，也无法查看真实内容，防止数据被管理员泄

密或者被黑客窃取。

如何在解决上述企业文档安全管理的同时，又不会降低企业的工作效率和文档使用的方便性，是建设现代企业电子文档存储与分发共享系统的新挑战。

2. 密九盘简介

密九盘是深圳奥联信息技术有限公司经过多年研发，用于提供安全电子文档管理与保护的系统，解决了企业文档数据在传输、存储与分发过程中的安全性。密九盘可以实时保护企业内部流向公有云和私有云的敏感文档数据，保护企业的隐私数据不被非法人员窃取。

密九盘有两种产品形态，在私有云模式下，密九盘提供一套专用的云数据安全分享系统解决企业内部电子文档存储与分发的安全性问题；在公有云模式下，密九盘提供一套 WEB 加密网关系统解决企业文档数据在第三方公有云盘（如百度云盘、115 网盘）的数据保密问题。

2.1. 私有云模式

密九盘的私有云系统是一套安全云存储、安全云分享的解决方案，全程加密保护。由 WEB 前端业务系统、WEB 后台管理系统、云盘加密网关、标识密码管理平台组成。

密九盘结构图：



2.2. 公有云模式

密九盘的公有云系统是在深刻理解企业客户在向云计算迁移过程中对保护企业敏感数据需求的基础上，推出的针对企业的云加密解决方案。本产品能够有效帮助企业解决在使用云平台保护防止敏感数据泄露等问题，既保证用户使用大众互联网产品的需求，也针对企业针对第三方云平台持有敏感信息泄露的担忧。相比于目前国内市场上的加密产品，密九盘产品的优势有以下几点：

- 不需要在终端安装任何的软件，且不改变应用软件的功能、流程和使用习惯，自动对用户的敏感数据提供自动的加密服务。
- 采用国家标准加密算法 SM9 对敏感数据进行加密，保证数据的安全。
- 目前提供了对云存储、私有应用数据加密保护的解决方案。密九盘系统支持透明网桥、网关 NAT 等多种部署模式。透明网桥模式的特点是无需更改客户网络拓扑的环境，极大的简化了部署方式。

3. 密九盘的系统组成

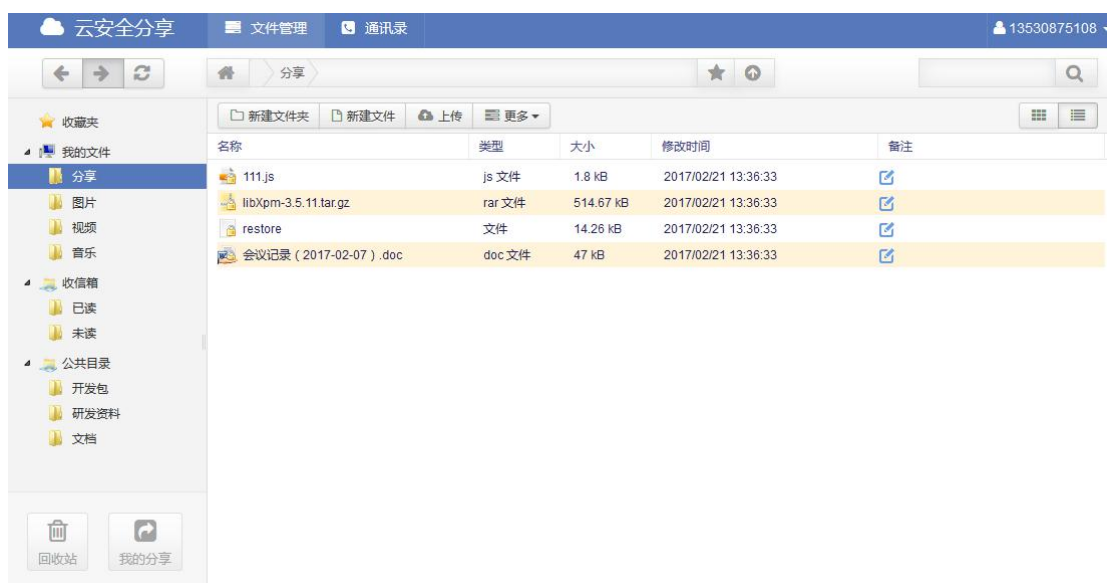
3.1. 私有云模式

3.1.1. WEB 前端业务系统

3.1.1.1. 业务系统简介

WEB 前端业务系统是密九盘的重要核心部分，界面仿照 windows 系统所设计，根据使用习惯设计功能，支持右键操作、拖拽、快捷键。如按 F2 重命名、DEL 删除文件/文件夹、ctrl+a 全选、ctrl+c 复制选中、ctrl+v 粘贴、ctrl+x 剪切，右键重命名，右键删除，右键打开等等，操作简单。

所有文件基于 SM9 的国密算法进行加密存储，支持加密分享。支持文件查找、备注、排序、图标列表切换等。



3.1.1.2. 我的文件

用于存储私人文件，可分享文件/文件夹给其 TA 人，让其 TA 人浏览到。

3.1.1.3. 收信箱

接收别人分享给自己的文件，可在未读或已读中查看。显示分享的时间，有效期，大小，短信通知接收人等等。

3.1.1.4. 企业公共目录

公共目录为本企业下所有用户可查看的区域，带有权限控制功能，默认不允许控制（包括编辑，删除，重命名等）别人的文件，公共目录管理员或者设置了赋权的用户除外。

3.1.1.5. 回收站

存储删除后的文件，避免了误删除的情况。

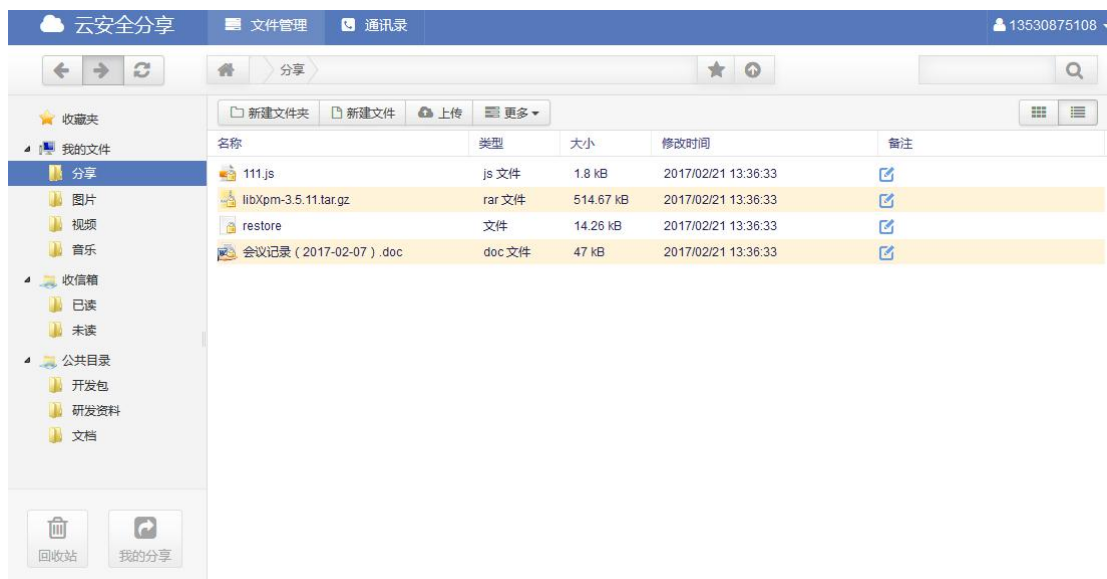
3.1.1.6. 通讯录

将常用的联系人添加到通讯录中，方便联系与分享文件。支持从企业联系人批量添加到通讯录中。

3.1.1.7. 我的分享

查看分享给别人的文件，支持分享文件的状态追踪。点击状态可查看到接收人用户标识、读取状态、读取时间、是否短信通知、短信结果等。

附业务系统功能图：



3.1.1.8. 文件管理

- 文件选择：单选，鼠标框选，shift 连选，ctrl 随意选择，键盘上下左右、home、end 选择。
- 文件操作：选择文件后，可以进行复制，剪切，删除，属性查看，压缩，重命名，打开预览等操作……。
- 文件上传：多文件批量上传；html5 拖拽上传(拖拽到窗口实现无缝上传)
- 右键功能：文件右键，文件夹右键，多选后右键操作，桌面右键，树目录右键操作，右键菜单绑定快捷键（全选——复制——剪切——粘贴——删除——重命名，设置……）。

- 文件浏览：列表模式, 图标模式；双击进入子文件夹；地址栏操作；打开文件夹记录逆势操作记录（前进后退）。
- 支持拖拽操作：选中后拖拽, 实现剪切到指定文件夹功能。
- 快捷键操作：delete 删除, ctrl+A 全选, ctrl+C 复制, ctrl+X 剪切, up/down/left/right/home/end 选择文件。

3.1.1.9. 在线预览

- 支持几乎所有编程语言的在线编辑(高亮, 多光标编辑. 堪比本地的 sublime)。
- 文件预览：文本文件内容查看编辑保存；html, swf 文件预览。
- 图片预览：自动生成缩略图, 图片幻灯片播放。
- 音频播放：在线播放音乐, 视频文件；支持 mp3, wma, mid, aac, wav; mp4, 。
- 视频播放：在线视频文件播放, 支持格式：flv, f4v, 3gp(需要搭建 office online 服务器)。

3.1.1.10. 在线编辑

- 支持 60 多种代码(数据文件)高亮。
- 支持多标签：同时编辑多份文件, 拖动标签可以切换顺序; 支持最大化模式。
- 主题切换：选择你喜欢的编程风格。
- zendcodeing 支持, 从此爱上在线编程。
- 查找、替换；撤销反撤销, 维持历史记录。
- 自动补全[], {}, (), "", ''；自动换行, 自定义字体, 代码折叠等诸多实用功能。

3.1.2. WEB 后台管理系统

密九盘提供完善的管理功能，方便管理员进行系统的维护、管理工作。具体管理菜单如下：

3.1.2.1. 首页

显示管理软件版本号、系统 CPU 负载、系统时间、内存使用、硬盘使用详情等。

3.1.2.2. 系统资源

查看系统 CPU 负载、系统内存使用、网络流量分析资源图，点击图可查看详细的 1 年、1 月、1 周、1 天的资源图，并进行网络流量分析。

3.1.2.3. 系统管理

配置 https, ssh 的端口号。

3.1.2.4. 设置时间

把本地系统时间同步到服务器; NTP 服务器时间同步到服务器。

3.1.2.5. 重启和关机

对服务器进行关机重启操作。

3.1.2.6. 备份恢复

在备份时可选择备份的数据内容(系统配置，系统数据)。如果用于不同机器之间的备份与恢复，一般不建议备份和恢复系统配置。

3.1.2.7. 网络接口

可对设备各个网络接口信息地址进行配置。

3.1.2.8. 路由设置

可对该设备的静态路由信息进行添加、编辑与删除操作。

3.1.2.9. DNS 设置

配置 DNS 域名解析服务器。

3.1.2.10. 分组管理

- 修改所选择的分组信息和该分组中的用户状态
- 添加、删除分组

3.1.2.11. 用户管理

- 查看选择的分组下用户信息
- 添加用户到指定的分组
- 修改用户基本信息、状态和分组信息
- 删除用户
- 公共目录指定管理员

3.1.2.12. 批量导入

按指定的状态和所属分组，批量导入上传文件中的用户标识。

3.1.2.13. 管理员账户

对选中分组的管理员进行添加，删除，编辑资料和修改登录操作。

3.1.2.14. 管理员日志

- 支持按管理员姓名查询日志信息。

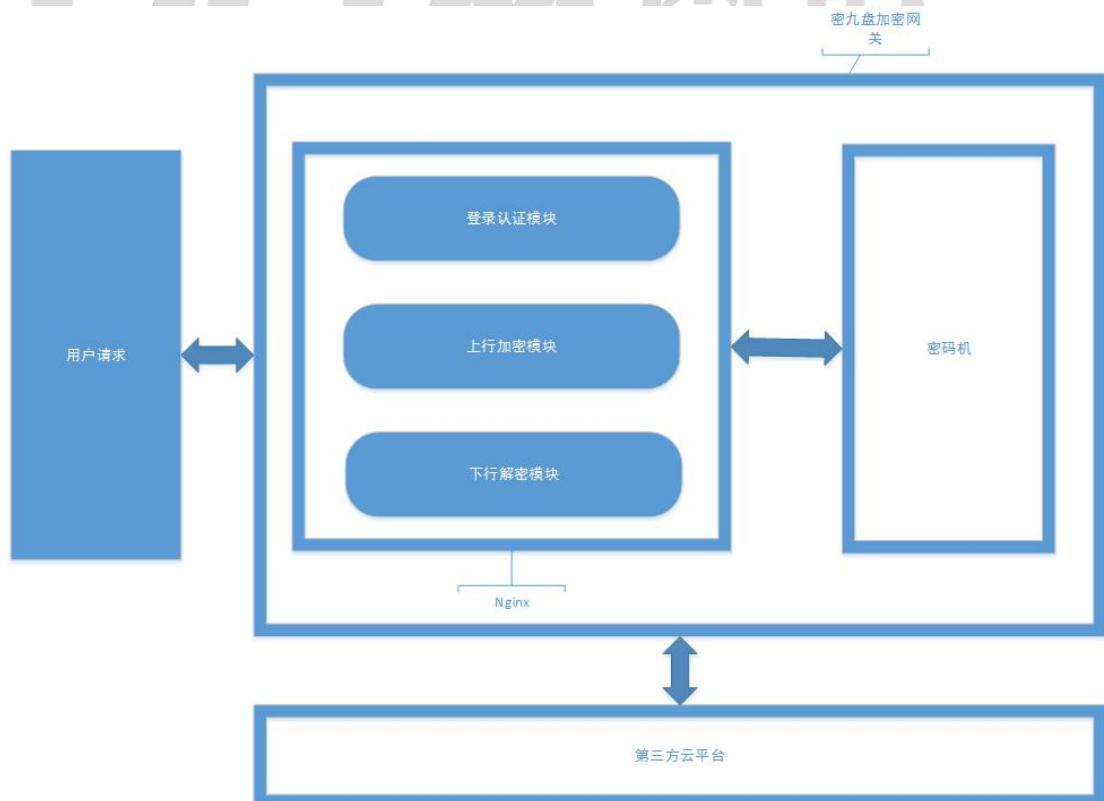
- 支持按操作查询日志信息
- 支持按操作状态查询日志信息
- 支持按创建时间查询日志信息
- 根据查询条件的组合可以详细查看管理员日志

3.1.2.15. 文件分享日志

- 支持按分享人查询历史日志信息
- 支持按接收人查询历史日志信息
- 支持按分享状态查询用户历史日志信息
- 支持按分享时间段查询用户历史日志信息
- 支持按文件的 SID 查询用户历史日志信息

3.2. 公有云模式

公有云模式系统组成有四大部分组成：



3.2.1. 登陆认证模块

通过分析 http 请求，将用户登陆第三方平台的状态记录（用户名，是否登陆成功）缓存。

3.2.2. 上传文件加密模块

对上传文件请求分析，用 sm9 加密算法将上传请求中的文件数据根据用户名进行加密。

3.2.3. 下载文件解密模块

对从第三方平台返回的文件数据进行分析，用 sm9 加密算法对其进行解密。

3.2.4. SM9 密码机

提供加解密服务，作为密九盘的加密部分。

4. 密九盘的功能

4.1. 私有云模式

4.1.1. 后台管理功能

4.1.1.1. 用户管理

用户的管理只需要轻松的点击，即可实现。如用户的增删改查，批量导入，用户停用等等。用户和分组显示一目了然。

查看用户：

4.1.1.2. 日志安全审计

管理员可以从管理员日志菜单中了解到，某某做了什么操作、时间段、IP地址，或者误操作了还可以从日志中恢复。

日志管理 >> 管理员日志

管理员日志查询

管理员: 操作: 所有操作 操作状态: 所有

时间: 至 操作内容: 查询

编号	管理员	ip地址	操作	操作内容	操作状态	创建日期
4	admin	192.168.1.51	用户管理	添加用户:用户标识:13512345678,描述:,状态:正常,所属分组:研发	成功	2017-02-20 10:21
3	admin	192.168.1.51	用户管理	添加分组:分组名称:测试,上级分组:root	成功	2017-02-20 10:19
2	admin	192.168.1.51	用户管理	添加分组:分组名称:研发,上级分组:root	成功	2017-02-20 10:19
1	admin	192.168.1.51	登录	admin	成功	2017-02-20 10:10

4.1.2. 文件安全管理功能

4.1.2.1. 文件/目录管理（上传、下载）

➤ 浏览器需求：支持浏览器：Chrome，Firefox 3+，Safari 5.2+，Opera 9+，IE 9+

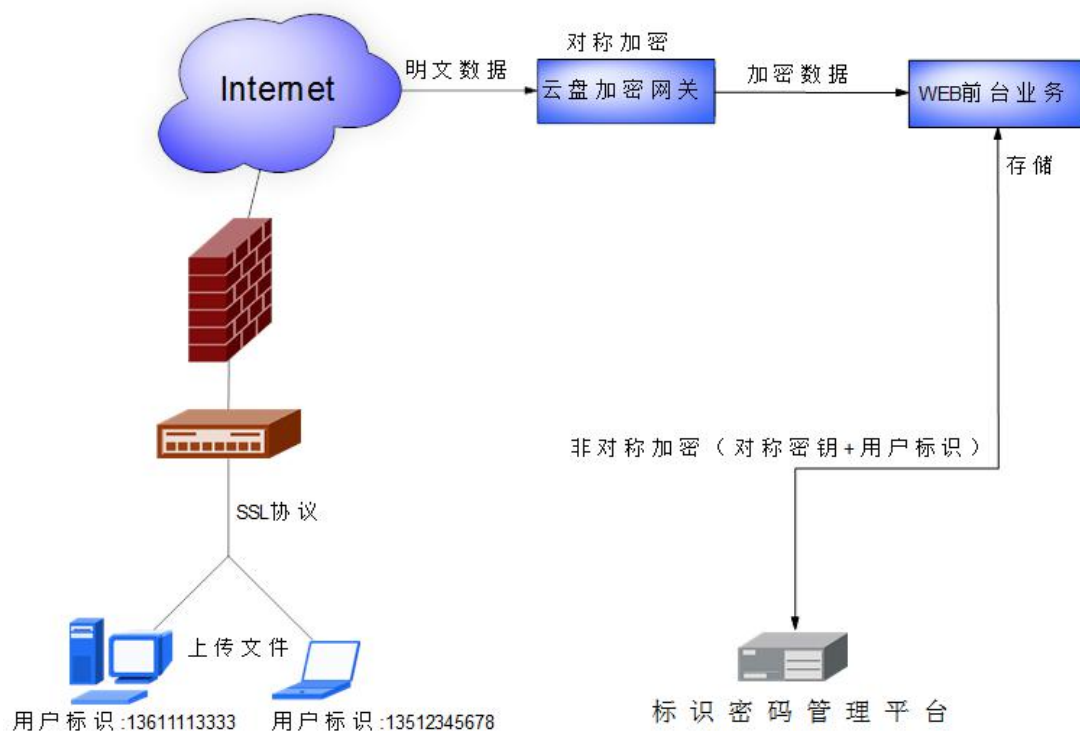
➤ 上传：支持拖拽上传，HTML5 & FLASH 上传，文件多选，分片与并发结合，将一个大文件分割成多块，并发上传，极大地提高大文件的上传速度。个别浏览器带支持带目录上传。禁止上传所配置的文件后缀名，如.php、.jsp 文件等。

上传过程通过云盘加密网关进行文件加密，前端业务系统接收到数据进行大文件合并，存储工作。

➤ 下载时会进行非对称解密，判断解密人是否有权限解密。只有解密成功才能下载文件。支持打包下载，边下边解密。

4.1.2.2. 文件加密存储

加密流程图



从流量图可看到，用户上传数据使用的 SSL 协议，当数据到达加密网关时数据加密，服务器将密文数据存储到硬盘上，同时对上传者（解密人）进行非对称加密。解密文件时，取出解密人对文件做对称加密。

4.1.3. 文件安全分享功能

加密文件被分享时，会进行非对称解密，取得对称密钥后，把新的接收人一起存入到解密列表里面，进行重新加密保存。

分享的文件会生成一个 64 位字符串做为唯一标识，根据此字符串才能找到对应的文件，除 64 位字符串外，还有一个对应的 6 位字符串密码。只有两者匹配成功才会进入到登陆验证的步骤。

分享的文件根据本域用户，外域用户，公共分享不同的类型有不同的验证情况，当验证成功并附合以下两种情况才能浏览文件。

被分享的文件只有符合以下两种情况才能解密

- 1) 接收人是否在接收列表里面，不在列表是没有权限查看的
- 2) 解密人在解密列表里面

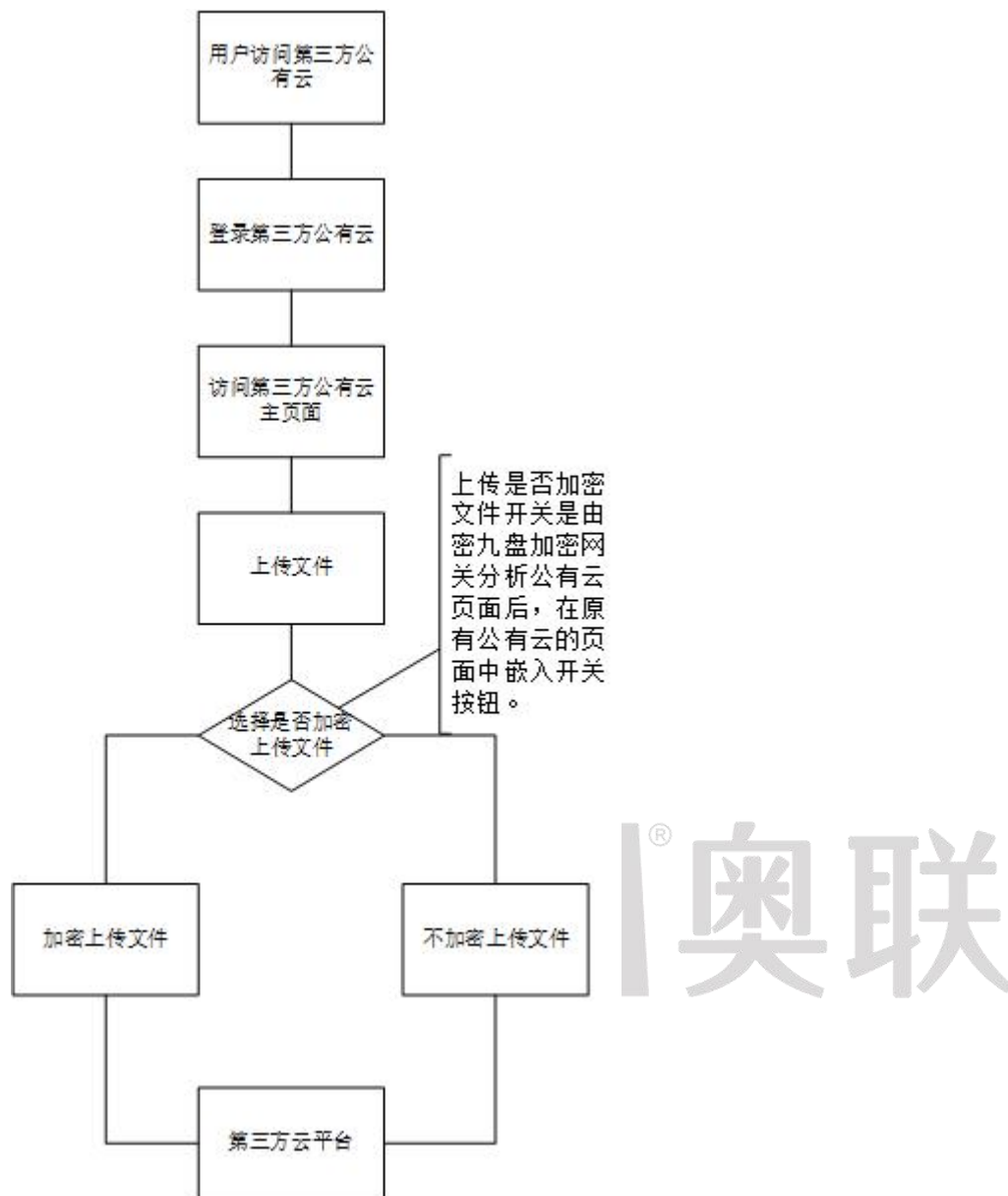
总结如下：

- 1) 每个分享的文件有唯一长标识，有对应密码
- 2) 是否为接收人，并且需要验证登陆
- 3) 是否在文件解密列表里面

4.2. 公有云模式

用户使用流程如下：

OLYM[®]奥联



4.2.1. 云盘文件加密

在使用第三方云盘上传文件时，系统会自动对文件进行加密，在请求到达第三方云盘时，请求中带的文件数据已经为密文。

4.2.2. 云盘文件解密

在使用第三方云盘下载文件时，系统会从第三方云盘取加密文件。会对第三方云盘的密文文件进行解密。

4.2.3. 无缝对接第三方云平台

在使用密九盘网关访问第三方云平台时，用户不会感知密九盘的存在。将保持原有云平台的界面和操作方式，用户不用学习，没有使用成本。

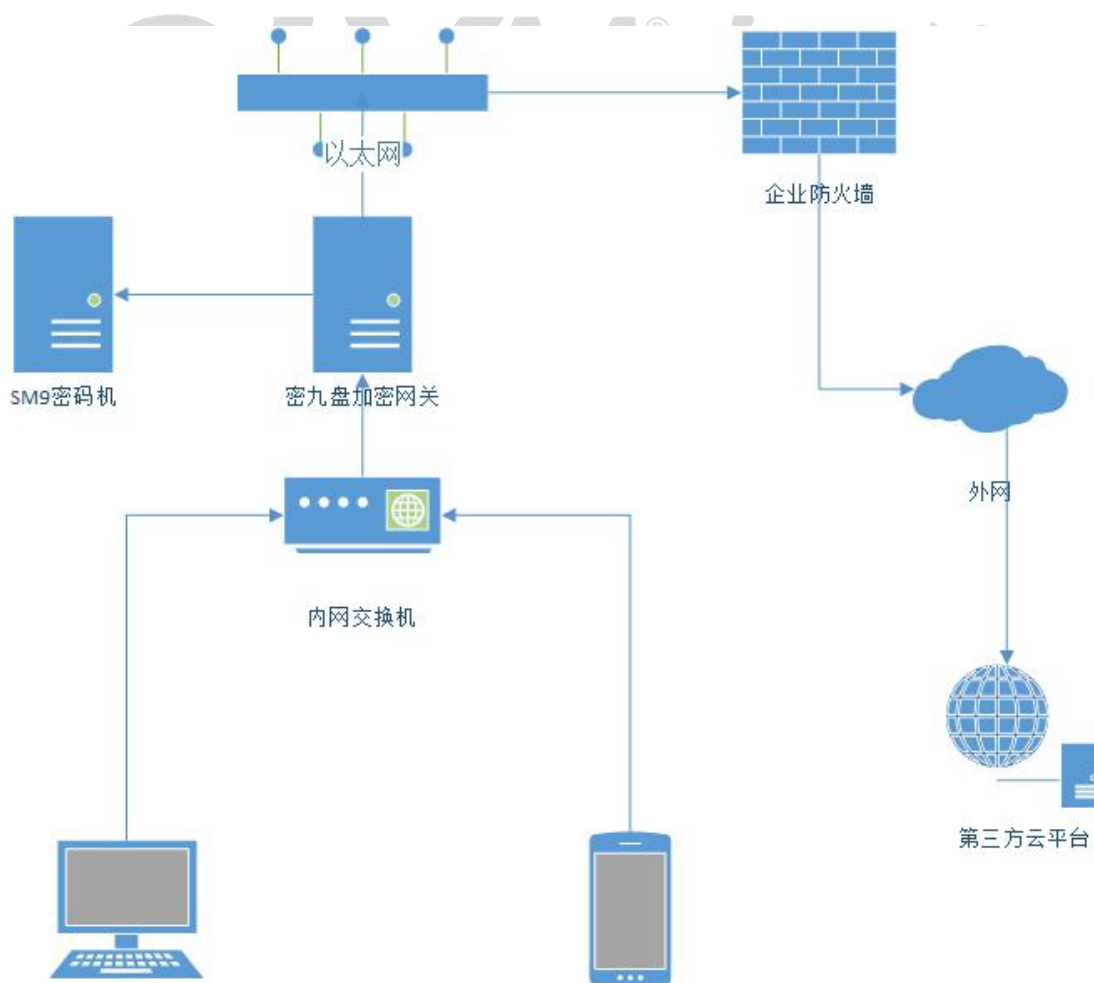
5. 部署方式

5.1. 公有云系统部署方式

5.1.1. 桥接模式

将内网交换机的所有流量导入密九盘加密网关，密九盘通过筛选端口和 URL 对指定的请求进行处理，将其它请求通过代理方式访问到外网。

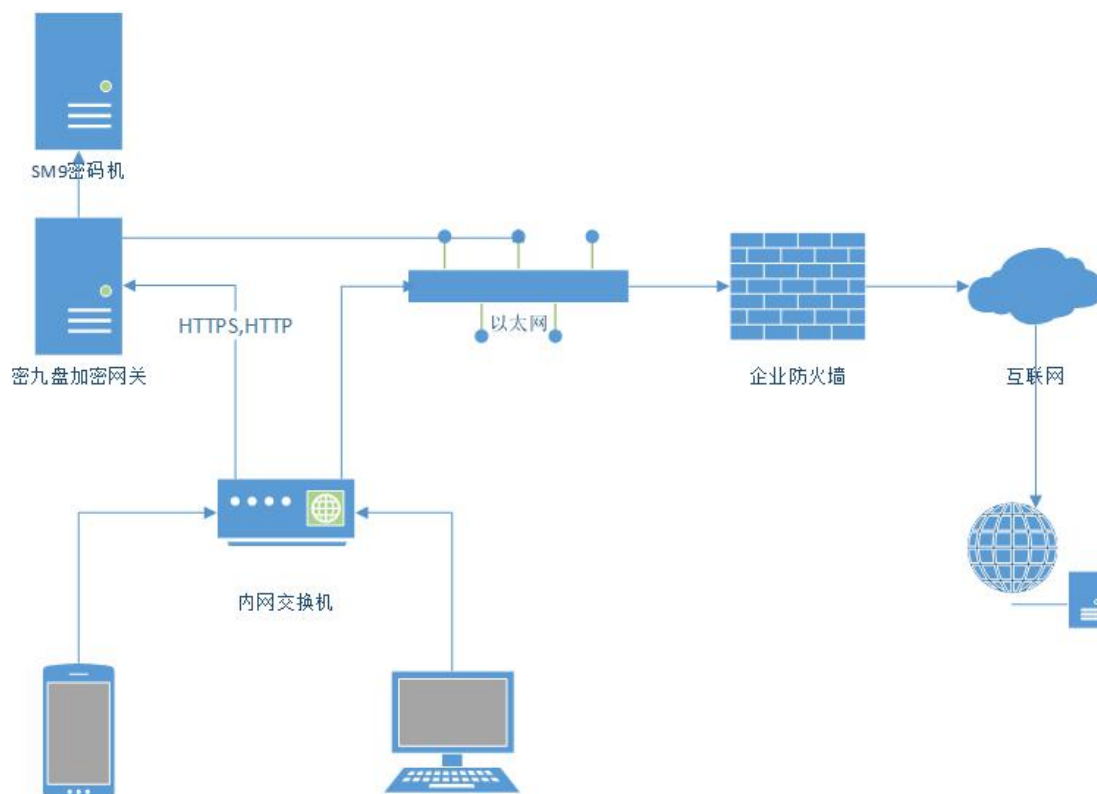
架构拓扑图如下：



5.1.2. 路由模式

通过配置路由器规则，将所有访问 **http** 和 **https** 的请求导入密九盘加密网管，密九盘加密网关对请求进行成立后代理访问第三方云平台。

架构拓扑图如下：



6. 密九盘的特点

6.1. 基于 SM9 的国密算法

传统的云储存或云分享系统没有采用密码技术或者简单的对称密码技术来进行数据存储与传输的保护，存在数据易泄露，易被攻击破解的风险，另外如何保证文档数据在分享或分发的同时也能做到加密保护，只有合法的授权人才能解密查看被保护的数据，也需要采用合适的密码技术方案；而传统的密码技术要么解密身份认证问题，要么解决数据加密问题，很难做到基于身份信息的策略授权加密，即使能做到，也需要结合多套密码系统，实现难度大，部署实施复杂。

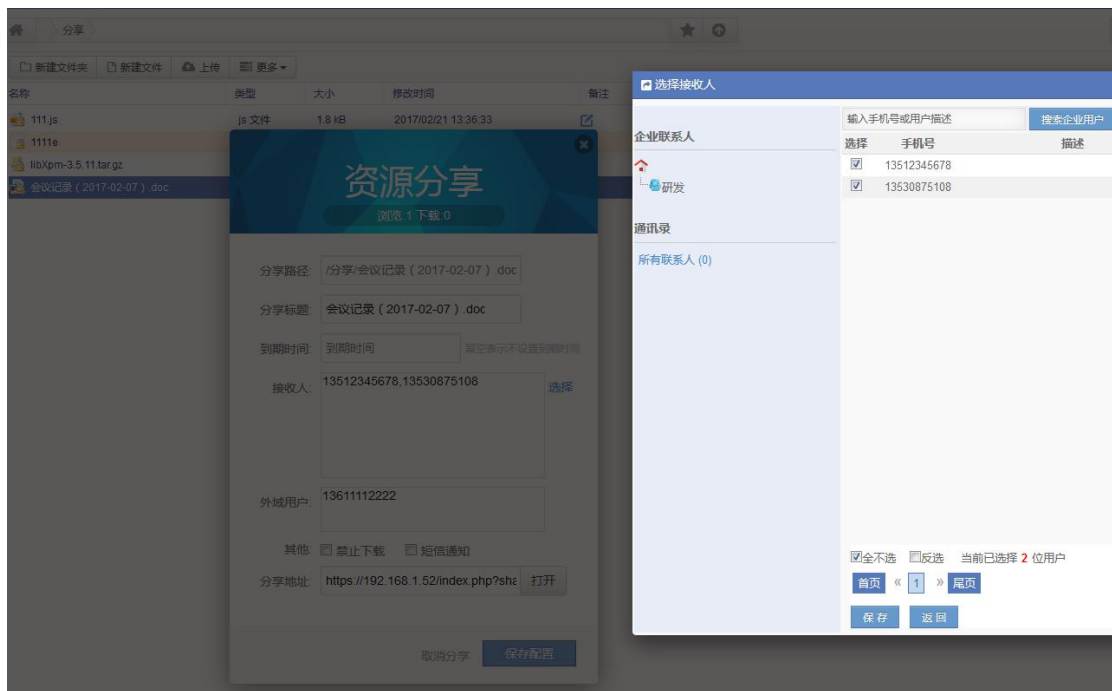
本方案中的密九盘系统采用了国家密码局发布的SM9标识密码算法这种新型密码技术，很好的解决了基于身份信息的策略授权加解密难题，在同一套密码系统中将身份认证与基于策略的数据加密有机结合在了一起，较大程度的降低了系统部署的复杂度，降低了用户使用的门槛；而且SM9密码技术是国家密码管理局发布的最新公钥技术标准，具有更高的自主安全可控性。

6.2. 文件安全管理、存储加密

- 密九盘支持使用密码认证登陆, SM9 认证 APP 扫码登陆，SSO 系统单点登陆。只有成功登陆的用户才能管理文件。被分享的文件只有阅读权限。
- 用户不能通过浏览器输入文件 URL 的方式来访问文件。
- 通过加密网关系统，使数据落盘即为密文，数据实时加密存储，非法用户无法获得有效数据
- 数据集中存储，便于安全管理，增强敏感数据访问可控性
- 加密的安全传输通道防止“中间人”截取数据
- 禁止动态语言脚本的执行，防范 XSS 跨站脚本，SESSION 攻击等，为系统保驾护航
- 数据分享，用户之间分享的信息也是密文形式，只有授权的用户才可见并获取真实内容
- 加密数据和明文数据大小一样，不用担心加密后数据变大

6.3. 文件安全分享、灵活方便

在密九盘中选择要分享的文件，右键选择分享，在弹出的页面中可选择接收人、外域用户、过期时间，短信通知等。分享后，接收人可浏览此文件。



- 本域分享（有接收人的）：是指本企业中的联系人，可通过收信箱查看收到的文件。也可通过短信通知打开 URL，使用账号密码验证进行文件的查看。
- 外域用户：是指非本企业中的，可通过短信通知打开 URL，使用短信验证码的方式验证并查看文件。
- 公共分享：指不选择接收人，不填入外域用户的分享。此分享只能通过复制 URL 发送给好友的方式进行查看。可以复制 URL 通过常用的联系工具，如 QQ、微信等发送给用户。

6.4. 云端密钥管理

传统的文件加密系统，需要在文件处理的终端侧集成密钥管理功能，处理逻辑较复杂，灵活性不够，同时也很难保证密钥数据在用户端存储的安全性。

本方案中的密九盘系统采用了在云端或网关侧进行数据加解密的技术，安全策略配置灵活，统一的密钥管理技术也能更好的保证密钥存储的安全性。