

密九令

基于国密算法的统一身份认证解决方案

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

版权所有 © 深圳奥联信息安全技术有限公司 2017-2020 保留一切权利。

本文档所涉及到的文字、图表等，版权归深圳奥联信息安全技术有限公司（以下简称奥联）所有，未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

名词解释

IBC: IBC (Identity-Based Cryptograph) 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	身份管理需求分析	1
第二章	技术方案	3
2.1	模块组成	3
2.1.2	SSO 服务器	4
2.1.3	增强认证网关服务器	4
2.1.4	IBC 平台	5
2.1.4	支持 OpenID 的应用系统	5
2.1.5	WEB 安全应用系统	5
2.2	技术原理	5
2.2.1	OpenID 模式	5
2.2.2	FORM 模式	6
2.2.3	即插即用模式	6
2.3	功能介绍	7
2.3.1	SSO 单点登录	7
2.3.2	连接远程服务器	9
2.3.3	系统配置功能	10
2.3.4	统一应用管理	11
2.3.5	增强认证网关服务器配置	13
2.3.5	统一身份管理	14
2.3.4	统一审计管理	15
2.3.6	应用系统防护功能	17
第三章	密九令部署	19
3.1.	部署方式	19
3.2.	应用系统整合	20
第四章	优势特色	21
4.1.	基于 SM9 的国密算法身份认证	21
4.2.	支持移动端扫描登录	21
4.3.	完美兼容传统的表单登录应用	21

4.4.	针对应用服务器的准入控制.....	22
4.5.	网络结构的零改造.....	22
4.6.	支持 RDP/SSH/VNC/TELNET 等远程应用协议.....	22
4.7.	使用 OPENID 协议实现单点登录.....	23
4.8.	完善的数据保护.....	23
第五章	扩展应用.....	24
5.1	SM9 算法简介.....	24
5.2	IBC 系列产品.....	25

第一章 身份管理需求分析

企事业单位经过多年的信息化建设，已经形成了一大批比较成熟的应用系统，其涉及的应用面覆盖了企事业的大部分生产或业务，例如：办公系统，人事系统，财务系统、信息管理系统、邮件系统、OA 系统、设备管理系统、ERP 系统等。由于历史原因，各应用系统都是在不同的时间段建设的，并且有可能是不同的应用厂商开发的，造成各个系统之间相互独立，身份认证不统一。每一个系统都需要用户输入当前系统的用户名和密码才能登录。随着业务的发展，企事业将来会增加到几十个应用系统在网上运行。尤其对于一些涉及业务较多的用户，如果每一个系统都需要他们进行密码的验证，那么用户使用系统的不便性是可想而知的。因此经常会有一些用户将多个系统设置成同一密码或是将记不住的密码写在纸上贴在桌子上，这样，对业务系统的访问存在着极大的安全隐患，增加了密码泄漏的风险，并且随着企业内控要求的加强，需要企业内部应用系统加强密码管理，每一个应用系统都需要在三个月内更换一次密码，记不住密码变得经常发生。而系统管理员的也被拖入了繁琐的重置用户密码的工作之中。

针对于上述情况，企事业单位需要建设一个单点登录平台，通过一次认证登录后就可访问所有有权访问的应用系统，避免频繁登录，并且能够保证用户身份的合法性和唯一性，对于应用系统的访问建立一套完整的安全防护和用户管理机制，实现以上功能需要考虑如下问题：

- 如何避免记忆多个密码？
- 如何避免频繁登录？
- 如何确保用户身份的唯一性，确保系统访问的安全性？
- 如何减少管理员花费在重置用户密码的时间？
- 如何为新建应用系统架构统一用户身份和认证平台？
- 如何对企业各应用系统的访问进行监控和跟踪，确保访问的安全性？
- 如何统一管理各个应用系统的服务器设备？
- 如何不更改用户应用程序的情况下实现上述需求？
- 如何不更改用户网络结构的情况下部署单点登录系统？

为了解决用身份管理的复杂性，采用单点登录方案，引入 SSO 系统。用户只需要登录一次就可以访问所有相互信任的应用系统。它无需用户记忆多个用户

名、密码，也无需用户进行多次登录访问应用系统。

- 从用户角度来看，单点登录解决了他们记忆多个用户名、密码的烦恼，解除了使用多个应用系统必须进行多次认证的重复劳动
- 从应用开发商角度来看，单点登录和统一认证使他们不必再开发身份认证模块，从而可以把更多精力投入到具体业务流程开发中。
- 从企业管理角度来看，单点登录和统一认证提高了员工的工作效率，减少了管理成本，提高了企业信息系统的的天性，也节约了后续开发系统的成本，提高了经济效益。

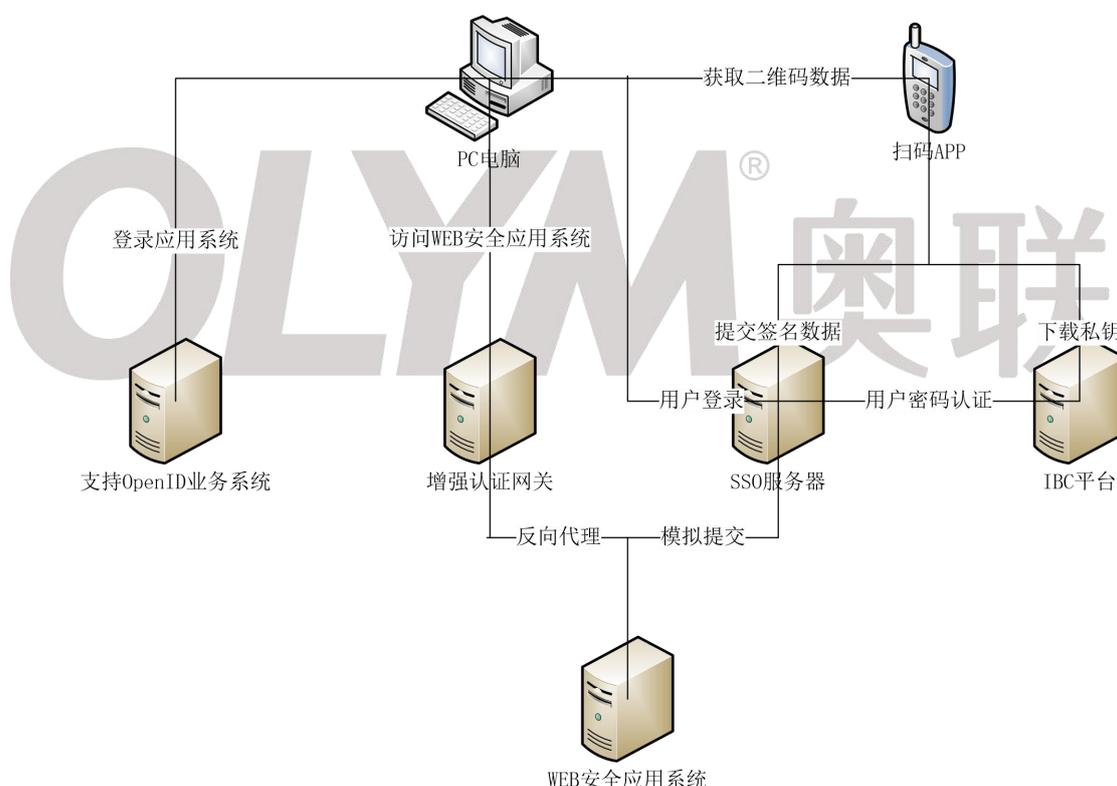
OLYM[®] 奥联

第二章 技术方案

密九令是基于标识密码(SM9)技术对 WEB 应用系统与系统远程管理 (SSH/远程桌面), 实现统一的账号管理、身份认证、权限管理和审计, 简化移动端认证和权限管理过程; 通过与移动端应用整合, 实现传输通道和数据加密。防止因应用系统漏洞、弱口令和中间人攻击等造成应用系统冒名越权访问和数据泄露, 加强应用系统的安全防范能力。

2.1 模块组成

密九令主要由手机扫码 APP、SSO 服务器、增强认证网关服务器、IBC 平台、应用系统组成, 各部分的具体关系如下图



2.1.1 扫码 APP

扫码 APP 用于移动端扫描登录, 主要包括如下功能:

- 在 IBC 平台注册用户并且下载私钥。
- 扫描 SSO 登录页面上的二维码, 获取二维码中的登录数据。
- 将登录数据用 IBC 平台下载的私钥签名后, 提交给 SSO 服务器进行验签。

2.1.2 SSO 服务器

SSO 服务器是密九令的重要核心部分，主要包括如下功能

- 安全登录功能：使用灵活的配置来满足不同级别身份认证的安全需求，保证用户登录 SSO 系统的合法性，同时也提供登录的便利性。登录配置如：用户名登录、扫码登录、用户名或扫码登录、用户名和扫码登录。
- OpenID 身份认证功能：业务系统可以通过标准的 OpenID 协议到 SSO 服务器进行身份认证，然后在安全的进入业务系统。
- 连接远程服务器功能：提供 WEB-SSH、WEB-RDP、WEB-VNC、WEB-TELNET 四种协议登录远程服务器，为运维人员维护服务器提供了极大的便利性。
- 即插即用功能：它对企业内部的业务系统的程序不需要修改，可以通过配置工作来实现单点登录，对于较为复杂的业务系统也可以开发独立的插件来实现，从而提高了密九令的适配性。
- 用户管理功能：对密九令用户进行管理、设置工作，例如：用户的添加、批量导入、禁用、修改密码等功能。
- 安全审计功能：系统记录了每一项操作的日志，方便管理员对某些异常行为的追踪，同时系统还对记录的日志进行了统计分析绘制成更直观的图表数据，方便管理员时刻了解系统的运行的情况。
- 账号托管功能：托管着用户应用系统的账号数据，对与每一条数据都采用不同的密钥进行加密存储。
- 系统配置功能：在 WEB 页面提供系统、服务器的各种配置修改，方便了管理员进行维护操作。

2.1.3 增强认证网关服务器

增强认证网关服务器是密九令的重要安全模块和实现即插即用功能主要模块，包括如下功能

- 拦截功能：拦截所有访问应用系统的请求，检查是否带了访问应用系统的合法 cookie 值。
- 验证登录状态功能：解析 SSO 服务器重定向传递过来的模拟登录业务系统登录后返回的信息，并且验证信息的正确性，正确则缓存登录信息，用于下次访问业务系统时验证请求的合法性，设置正确的 cookie 值，

访问应用系统

- 反向代理功能：对所有访问业务系统合法的 URL 则反向代理到业务系统服务器，从而使用即插即用功能可以对用户的网络实现零改造。

2.1.4 IBC 平台

扫码 APP 需要用标识私钥才能对二维码中的登录数据进行签名，并且密九令可以将自己的用户托管到 IBC 平台，所以 IBC 平台负责如下如下功能

- 标识私钥的产生和下载。
- 密九令系统用户的托管，提供用户状态查询、用户密码验证接口。

2.1.4 支持 OpenID 的应用系统

支持标准的 OpenID 身份认证，可直接通过 OpenID 接入密九令，实现单点登录需求。

2.1.5 WEB 安全应用系统

不支持 OpenID 身份认证，可以通过 SSO 服务器的即插即用功能实现单点登录需求。

2.2 技术原理

密九令摒弃了传统的单点登录实现方式，采用 OpenID 身份认证实现，相对于传统的共享 cookie 的方式更加安全和便捷。密九令目前支持 3 种模式的单点登录，即 OpenID 模式、FORM 模式、即插即用模式。三种模式的实现原理都各不一样，具体如下介绍。

2.2.1 OpenID 模式

这种 SSO 实现的原理是，SSO 服务器支持标准的 OpenID 身份认证，需要对已有的应用系统进行改造，使原有的应用系统支持 OpenID 身份认证，以后新建的应用系统也需要支持 OpenID 身份认证，基本实现流程如下

- a) 用户登录应用系统，应用系统返回 HTTP 重定向到 SSO 服务器，重定向的 URL 要传递 OpenID 协议的参数。
- b) 如果没有登录密九令则登录密九令，如果已经登录过了直接到下一步。

-
- c) SSO 服务器获取重定向的 OpenID 协议参数，生成当前 SSO 用户在此应用系统中的 Id Token，在返回 HTTP 重定向到应用系统，重定向 URL 要传递 Id Token。
 - d) 应用系统获取重定向的 Id Token，使用应用系统在 SSO 服务器中生成的密钥验证 Id Token 签名的有效性。
 - e) 验证 Id Token 签名有效，则解析 Id Token，验证 Id Token 数据项的有效性。
 - f) 获取 Id Token 中的用户名，登录应用系统成功。

2.2.2 FORM 模式

这种 SSO 实现原理是，SSO 服务器支持模拟登录，能托管应用系统的账号数据，不需要对应用系统的进行任何改造，但是有可能需要对现有的网络结构做改造，密九令系统和应用系统需要在同一个二级域名情况下才能工作，基本实现流程如下

- a) 用户登录密九令系统。
- b) 在密九令主页上点击要访问的应用系统，SSO 服务器获取应用托的账号、口令数据，如果没有托管账号，则需要用户输入，SSO 服务器用获取的账号、口令模拟登录到应用系统。
- c) SSO 服务器将模拟登录返回的 cookie、location 数据后，返回 HTTP 重定向到应用系统，重定向的 URL 为 location，并且设置获取的 cookie 到二级域名下。
- d) 重定向到应用系统后，应用系统可以获取到 SSO 服务器模拟登录的 cookie 后，判断当前 cookie 值已经登录，则用户登录应用系统成功。

2.2.3 即插即用模式

这种 SSO 实现原理是，SSO 服务器支持模拟登录，能托管应用系统的账号数据，需要增强认证网关拦截应用系统的所有请求，设置请求应用系统的 cookie 值，对所有应用系统的请求反向代理到真实的应用系统服务器。不需要对业务系统的代码进行任何改造，基本实现流程如下

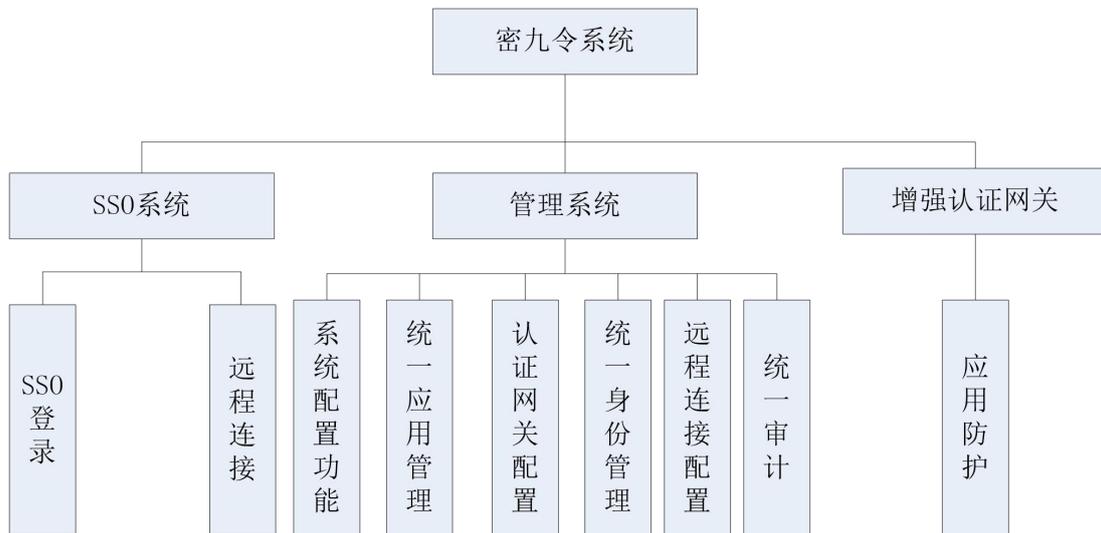
- a) 用户登录业务系统，增强认证网关检查没有登录当前业务系统，增强认证网关返回 HTTP 重定向到 SSO 服务器，重定向的 URL 要传递自定义

协议的参数。

- b) 如果没有登录密九令系统则登录密九令系统，如果已经登录过了直接到下一步。
- c) SSO 服务器获取重定向的自定义协议参数，获取当前 SSO 用户托管的业务系统账号，如果没有托管账号，则需要在页面上输入，SSO 服务器用获取到的用户名、密码模拟登录到业务系统。
- d) SSO 服务器将模拟登录返回的数据（cookie、location）封装成自定义协议数据，在返回 HTTP 重定向登录业务系统，重定向 URL 要传递自定义协议数据，增强认证网关验证自定义协议数据签名的有效性。
- e) 增强认证网关验证签名有效，则缓存自定义协议数据中的 cookie 数据，返回 HTTP 重定向要业务系统，重定向 URL 为自定义协议数据中的 location，并且设置重定向的 cookie 值为自定义协议数据中的 cookie 值。
- f) HTTP 重定向访问业务系统，增强认证网关检查已经登录当前业务系统，则反向代理到真正的业务系统。

2.3 功能介绍

密九令的功能结构如下图



2.3.1 SSO 单点登录

用户只需要登录一次密九令就可以访问所有接入的应用系统。

打卡密九令登录界面，如下图：



登录成功后显示即插即用应用列表，如下图：

密9令 15070964145，您好，欢迎登录SM9增强身份认证系统！【退出系统 修改密码】

上一次登录时间：2017-02-10 13:54:39
上一次登录IP地址：192.168.1.70
上一次登录地理位置：内网IP
上一次登录终端：PC端

B/S应用
C/S应用

应用名	应用状态	登录用户	是否可登录	上次登录时间	上次登录IP	上次登录位置	上次登录终端
cornail邮局	启用	huangqy@myibc.net	启用	2017-01-18 10:03:20	192.168.136.156	内网IP	PC端
CSS呼叫中心	启用	xkbao	启用	2017-01-18 11:17:50	192.168.136.156	内网IP	PC端
邮件探针	启用	admin@admin.com	启用	2017-02-06 15:12:35	192.168.1.74	内网IP	PC端
邮件探针	启用	huangqy@myibc.net	启用				
禅道	启用	chineyhuang	启用	2017-02-10 13:55:21	192.168.1.70	内网IP	PC端
富通OA	启用	linss	启用	2017-01-18 09:45:01	192.168.1.74	内网IP	PC端
wiki	启用	test	启用	2017-02-10 13:55:49	192.168.1.70	内网IP	PC端
集时呼叫	启用	--	--	--	--	--	
云分享	启用	15070964145	启用	2017-02-10 13:46:57	192.168.1.70	内网IP	PC端

选中禅道系统，首次登录时需要绑定应用账号，如下图：

密9令 禅道登录

温馨提示：

首次通过SM9增强身份认证系统登录禅道时，需要输入禅道的用户名和密码

修改了禅道的登录密码后，再次通过SM9增强身份认证系统登录禅道时，需要重新输入禅道的用户名和密码

禅道登录

用户名：

密码：

输入应用系统的账号、口令后即可单独登录禅道系统，如下图：



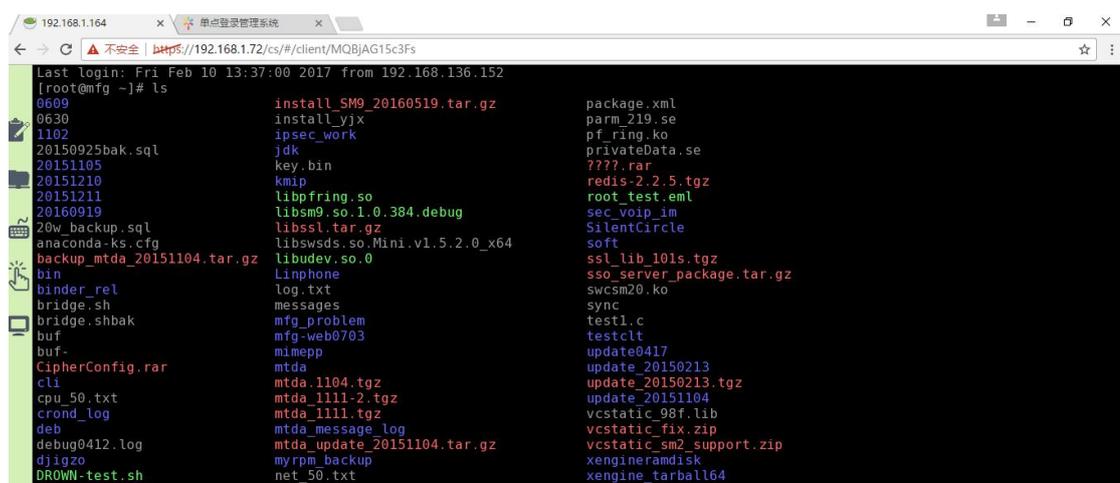
2.3.2 连接远程服务器

密九令系统不仅可以单点登录应用系统，还可以单点登录后连接远程服务器。

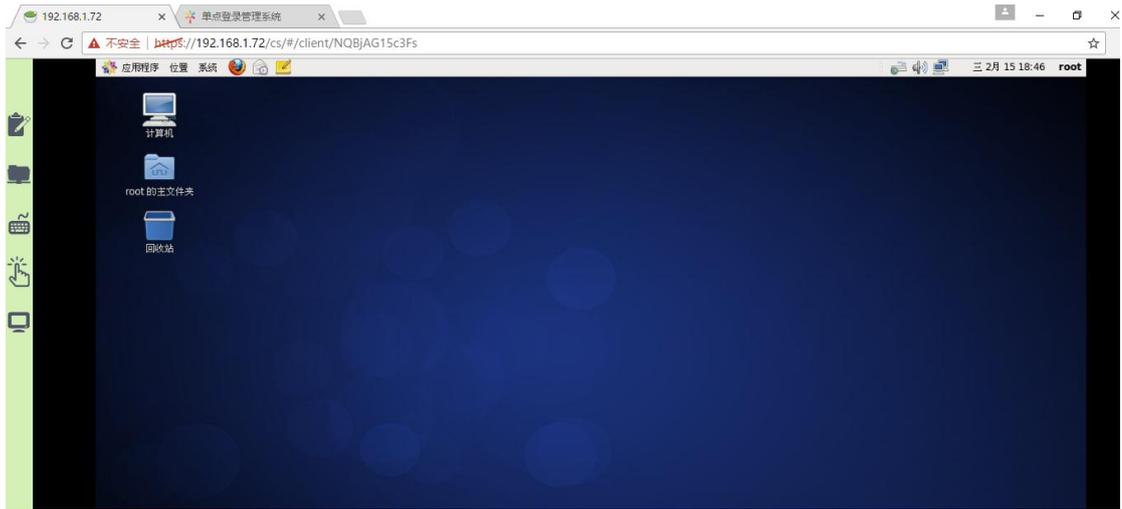
登录密九令后选中 C/S 应用，显示远程连接的服务器，如下图：



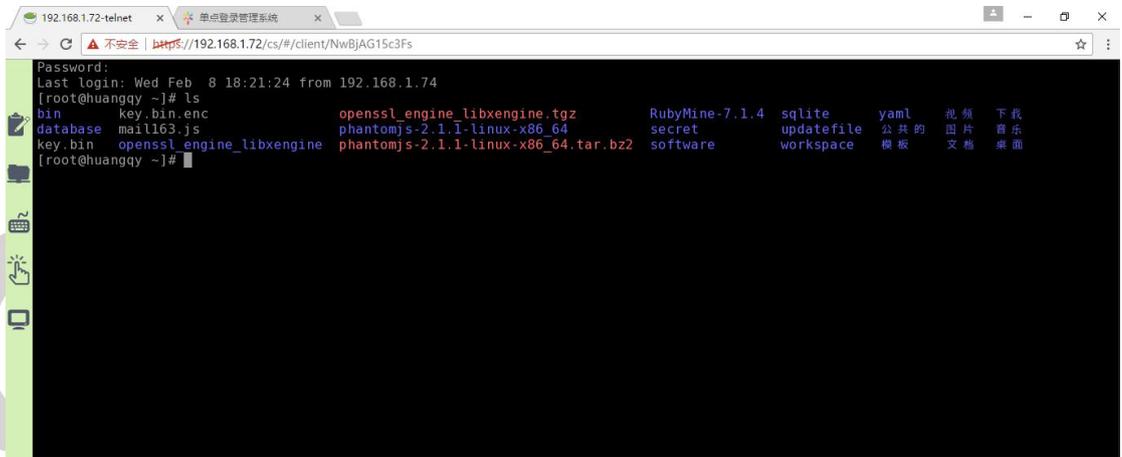
SSH 协议通过 B/S 模式连接远程服务器，如下图：



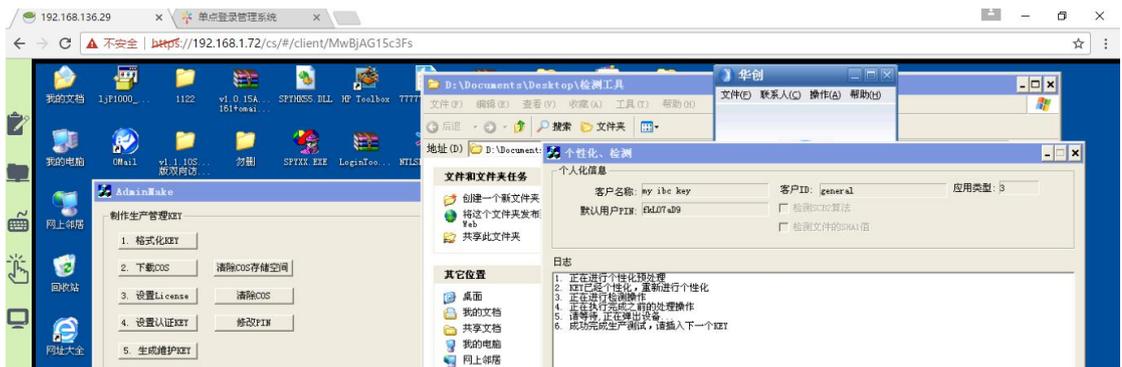
VNC 协议通过 B/S 模式连接远程服务器，如下图：



TELNET 协议通过 B/S 模式连接远程服务器，如下图：



RDP 协议通过 B/S 模式连接远程服务器，如下图：



2.3.3 系统配置功能

密九令提供完善的系统配置，方便管理员进行系统的维护、管理工作。具体配置工作如下：

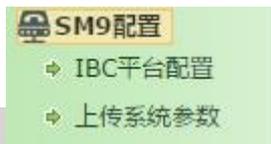
- 系统配置功能，如下图：



- 参数配置功能，如下图：



- SM9 配置功能，如下图：



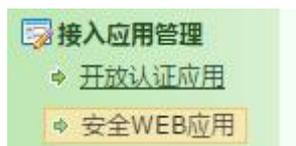
- 网络配置功能，如下图：



2.3.4 统一应用管理

对需要接入密九令的应用系统进行基本管理，如查询、新增、编辑、删除、禁用等操作，对于 OpenID 应用还提供密钥更新、查看功能。

统一应用管理分为：开放认证应用（OpenID 应用）、WEB 安全应用，如下图：



OpenID 应用列表，如下图：

接入应用管理 >> 开放认证应用

条件查询

应用ID: 应用名:
 应用状态: [所有] 创建时间: 至

应用ID	应用名	回调url	创建时间	操作
nginx_auth	认证网关		2017-01-13: 17:37:00	[禁用] [删除] [编辑] [更新密钥] [查看密钥]

第 1 / 1 页, 共有 1 条记录 < 上一页 下一页 >

WEB 安全应用列表，如下图：

接入应用管理 >> 安全WEB应用

条件查询

应用名: 应用状态: [所有]
 创建时间: 至

应用名	应用状态	部署方式	创建时间	操作
cornall邮局	启用	有认证网关	2017-01-13: 17:42:50	[禁用] [删除] [编辑]
CSS呼叫中心	启用	有认证网关	2017-01-13: 17:44:44	[禁用] [删除] [编辑]
邮件探针	启用	有认证网关	2017-01-13: 17:46:43	[禁用] [删除] [编辑]
神道	启用	有认证网关	2017-01-13: 17:48:13	[禁用] [删除] [编辑]
富通OA	启用	有认证网关	2017-01-13: 17:49:57	[禁用] [删除] [编辑]
wiki	启用	有认证网关	2017-01-13: 17:51:59	[禁用] [删除] [编辑]
定时呼叫	启用	有认证网关	2017-01-13: 17:53:57	[禁用] [删除] [编辑]
云分享	启用	有认证网关	2017-01-13: 17:55:10	[禁用] [删除] [编辑]

第 1 / 1 页, 共有 8 条记录 < 上一页 下一页 >

OpenID 应用新增页面，如下图：

接入应用管理 >> 开放认证应用 >> 添加应用

应用ID: * 应用ID由字母或数字组成,长度3-64位,不支持特殊字符!

应用名称: *

状态: 启用 禁用

验证算法: HS256

回调URL:

备注:

WEB 安全应用新增页面，如下图：

应用管理 >> 安全WEB应用 >> 添加应用

应用名称: *

状态: 启用 禁用

LOGO上传: 未选择任何文件

部署方式: 有网关认证

对外服务URL: *

登录方式: 表单提交

登录提交URL: * 默认URL

登录页面URL: *

登录提交参数: *

匹配成功信息正则表达式: *

说明: 用户名、密码、验证码请分别用占位符: .password、.verifyCode代替, 例: operatorCode=user&password=password&encode=verifyCode&loginType=0

2.3.5 增强认证网关服务器配置

提供增强认证网关的主要配置，和各个应用系统的配置，如下图：



认证网关主要配置，如下图：

认证网关配置 >> 全局配置

memcached服务器地址：	127.0.0.1:8888	* 例：127.0.0.1:8888
redis服务器的地址：	127.0.0.1:6379	*
redis服务器的登陆密码：	*****	获取密码
SSO服务器地址：	192.168.1.72	* 获取地址
SSO服务器端口：	443	* 自动获取默认为443端口，如果不是，请手动修改
应用ID：	nginx_auth	*
主密钥：	*****	* 获取密钥
PIN码：	*****	*
slot：	***	*

修改 高级选项

应用管理列表显示，如下图：

认证网关配置 >> 应用管理

应用ID	应用名	对外服务地址	对外服务端口	对内服务地址	对内服务端口	匹配登陆URL	匹配退出URL	操作
LblT34	cormail邮局	192.168.1.72	1443	mail.myibc.net	80	/	/coremail/logout.jsp	[编辑] [删除]
Tl72qN	富通OA	192.168.1.72	5443	121.35.243.82	80	/	/logout.jsp	[编辑] [删除]
UpndcZ	wiki	192.168.1.72	6443	192.168.1.130	80	/		[编辑] [删除]
XbYchh	云分享	192.168.1.72	9443	192.168.1.26	443	/		[编辑] [删除]
ZDBWFA	禅道	192.168.1.72	4443	192.168.1.249	80	/	/zentaopms/www/user-logout.html	[编辑] [删除]
cuG1bR	CSS呼叫系统	192.168.1.72	2443	192.168.120.205	80	/	/admin/adminLogout.do	[编辑] [删除]
kF5cY	集时呼叫	192.168.1.72	7443	192.168.120.204	80	/		[编辑] [删除]
oaxeoh	邮件探针	192.168.1.72	3443	mail.myibc.net	5443	/	/users/logout	[编辑] [删除]

添加

新增应用，如下图：

认证网关配置 >> 添加应用

应用名

应用ID： 选择 * 由字母或数字组成,长度3-64位,不能带空格或其它特殊字符

应用名：

对外服务配置

地址： * 例：mail.myibc.net

协议： http协议 https协议

端口： *

本机服务配置

端口： 默认情况下与对外服务配置的端口一致

对内服务配置

地址： * 例：114.255.178.231

协议： http协议 https协议

端口： *

登陆退出配置

匹配登陆URL： 例：/user/ 添加

匹配退出URL： 例：/user/logout.png

添加 返回

2.3.5 统一身份管理

密九令系统不仅存储着自己账号、口令，同时也托管着应用系统的账号、口令。如下图：



对自己账号口令，主要提供如下功能

- 增、删、改、查功能。

查询功能，如下图：



新增功能，如下图：



- 批量导入功能，如下图：



对于应用系统托管的用户、口令主要提供如下功能

- 查询、删除、新增绑定

查询功能，如下图：

用户管理 >> cormail邮局用户

条件查询

应用账户： SSO账户：

用户状态： 注册时间： 至

序号	应用账户	SSO账户	创建时间	上次登录时间	上次登录IP	上次登录地区	备注	操作
1	huangqy@myibc.net	15070964145	2017-01-13: 18:13:57	2017-01-18: 10:03:20	192.168.136.156	内网IP		[禁用] [删除]
3	huangqy@myibc.net	huangqy@myibc.net	2017-01-16: 10:55:40					[禁用] [删除]
5	wangyh@myibc.net	18201568113	2017-02-09: 10:40:39	2017-02-09: 10:40:39	192.168.1.70	内网IP		[禁用] [删除]

第 1 / 1 页, 共有 3 条记录 < 上一页 下一页 >

新增绑定功能，如下图：

用户管理 >> cormail邮局用户 >> 新增绑定

SSO账号： *手机号码或邮件地址(需要在SSO用户中已经存在)

应用账号： *(最多50个字符)

应用账号密码： *

状态： 正常 禁用

备注：

● 批量导入功能，如下图

用户管理 >> cormail邮局用户 >> 批量导入

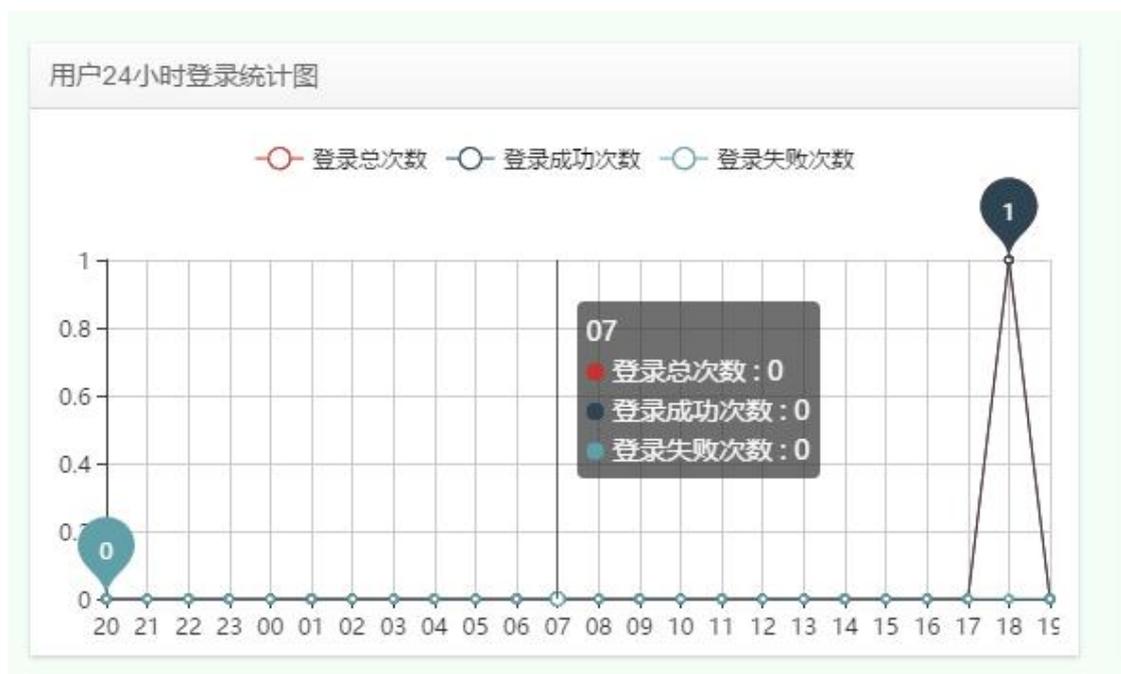
上传文件： 未选择任何文件 *文件后缀为.xls [下载文件模板\(右键另存为\)](#)

状态： 正常 禁用

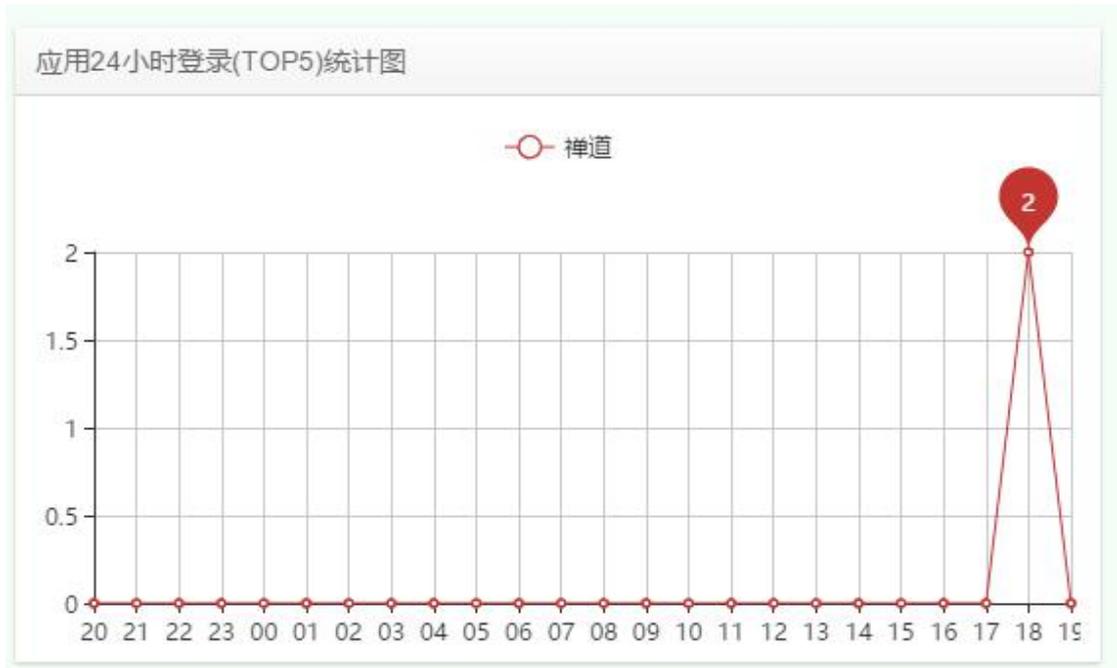
2.3.4 统一审计管理

密九令对系统运行的日志信息进行了定时统计，并且以图表的形式展现出来，让用户时刻了解系统的运行状态。

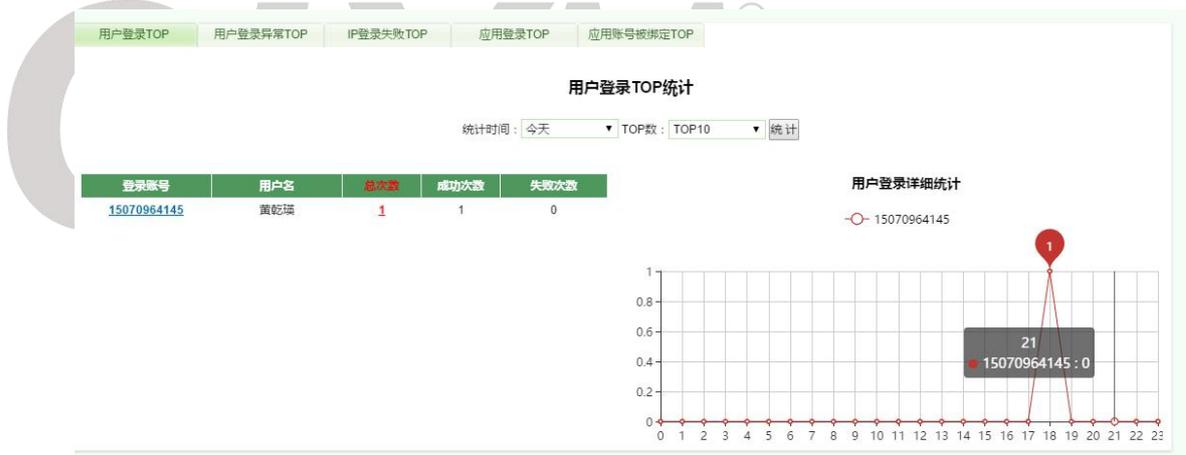
● 用户 24 小时登录次数的统计，如下图：



- 应用 24 小时登录的 TOP5 统计，如下图：



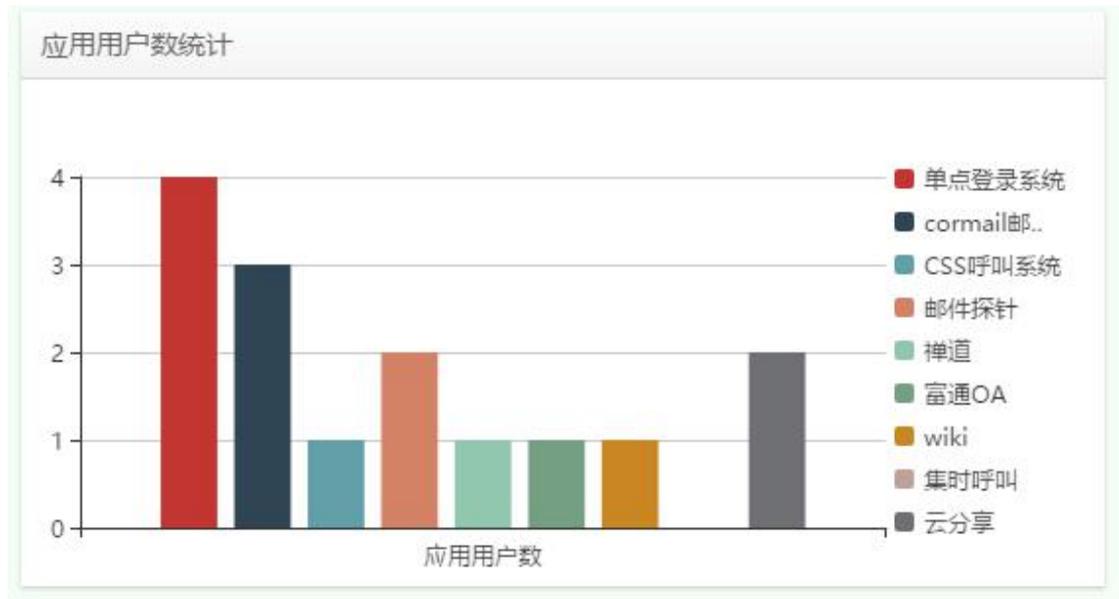
- 一些异常信息的统计，如下图：



- 设备的运行状态图



- 应用托管账号数量的统计，如下图：



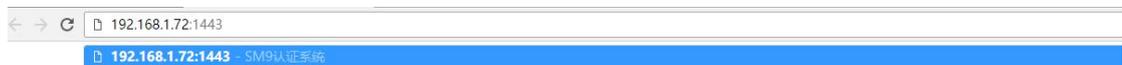
- 提供详细的日志查询，方便追踪痕迹，如下图：



2.3.6 应用系统防护功能

密九令通过增强认证网关，拦截所有的应用系统请求，检查必须经过安全身份认证才能进入应用系统。

访问应用系统，如下图：



应用系统没有安全身份认证，被增强认证网关拦截，并强制重定向到 SSO 服务器，如下图：



应用系统安全身份认证后，经过增强认证网关，进入应用系统，如下图：



OLYM[®] 奥联

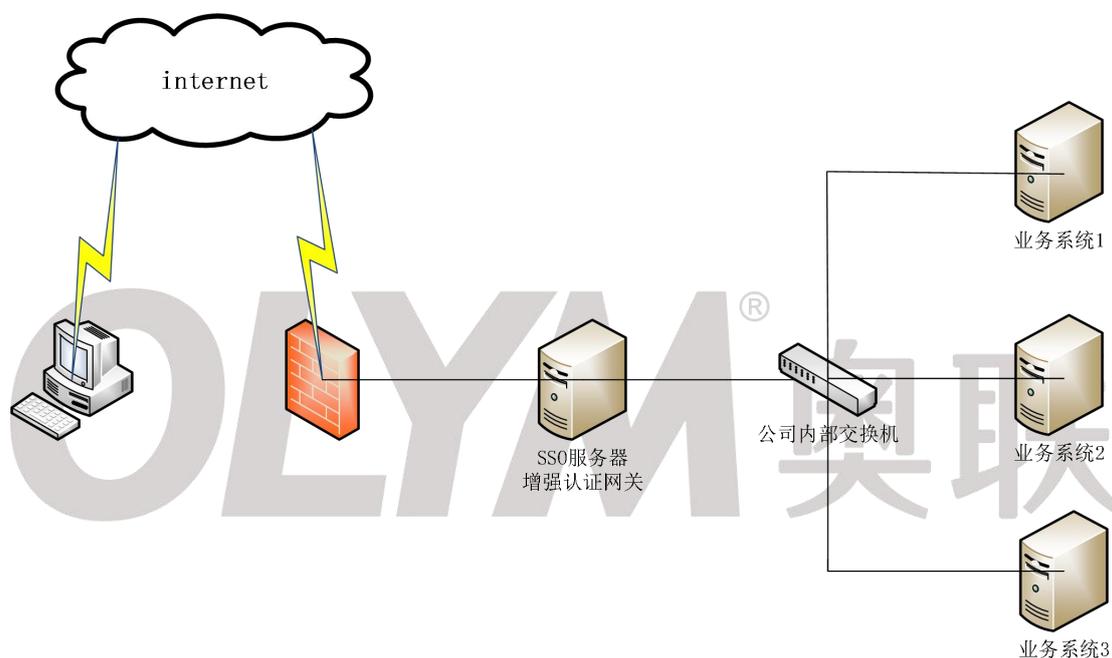
第三章 密九令部署

密九令的部署方式非常简便，可以对原有的应用系统不做任何改造，对原有的网络结构做任何的变动。但是为了提高系统的安全性，建议应用系统都放在内网，只对外放开放 SSO 服务器、增强认证网关服务器。

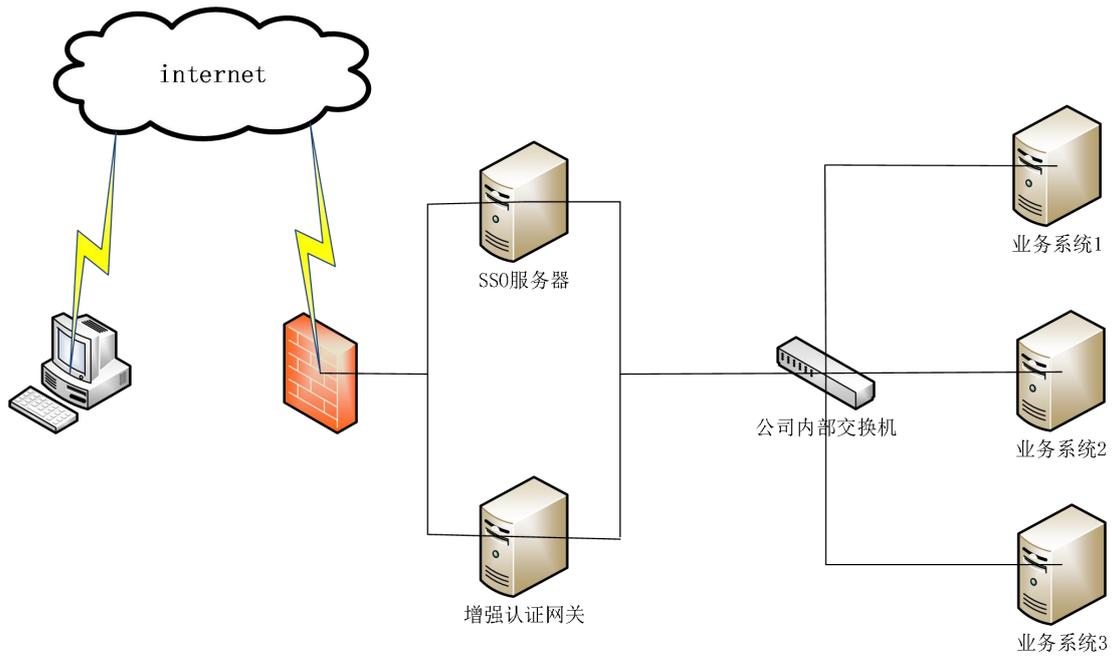
3.1. 部署方式

密九令系统的部署方式分两种模式：

1、增强认证网关和 SSO 服务器在同一台服务器上，如图：



2、增强认证网关和 SSO 服务器在不同的服务器上，如图：



3.2. 应用系统整合

企业单点登录的需求一般是已经建立了多个业务系统，而且开发公司不一，开发平台不一，互相形成了独立的异构系统。传统的单点登录解决方案需要对原有系统进行改造才能实现，但是由于企事业单位所建系统时间已久，有些原开发公司已无法找到相关的人员进行配合改造，因此，经常是单点登录工程拖的时间久，花费的钱无法预计，经常做到一半时已无法进行下去。并且开发改造严重影响了原有业务系统操作人员的工作。

密九令根据国内企事业单位这种现状，提出了全新的完善的解决方案，对原有系统不改造，采用填写配置的方式来将原有业务系统与密九令系统进行结合，实现单点登录。

密九令系统也为后续建设的业务系统提供了一个简单、安全的统一身份认证平台。后续建设的系统只需要按照 OpenID 身份认证的标准流程即可安全身份认证实现单点登录。

第四章 优势特色

在广泛研究客户需求的基础上，公司在安全行业多年经验的积累下，开发出了密九令安全身份认证产品。该产品具有以下特点：

4.1. 基于 SM9 的国密算法身份认证

扫码 APP 的签名私钥使用了 SM9 国密算法生成，目前 SM9 国密算法是安全性最高的商用算法，从数据安全上保证了密九令身份认证的安全性。

4.2. 支持移动端扫描登录

传统的基于用户、密码的身份认证方式一直被认为是不安全的，设置简单的密码很容易被攻击者破解掉，设置过于复杂的密码增加了用户的记忆难度，为了能够方便的记忆各种系统的密码，用户常常会将各种应用的密码设置成一致的，增加了撞库的风险，还要面对层出不穷窃取用户密码信息的钓鱼网站。

使用移动端基于签名和验签的方式扫描登录，能有效的避免上面的类似问题，从方式上提升密九令系统身份认证的安全性。不仅如此，密九令系统还针对扫描登录做了很多安全方面的工作，例如：扫描 APP 签名库的加固，签名私钥由 IBC 平台独立生成和分发，SSO 服务器使用独立封装的验签模块，从多个方面保证扫描登录不仅方便，还非常的安全。

4.3. 完美兼容传统的表单登录应用

由于企事业的每个应用系统都有可能是在不同时期、不同厂家开发的，当部署单点登录系统时不得不面对的就是如何兼容已有的历史系统，但是大部分的情况是，对已有的历史系统进行改造，但是改造的过程中面对的诸多困难也是可想而知的，所以企事业都希望能有一款单点登录产品能够很好的兼容历史，尽量少改造甚至不改造的前提下能够实现单点登录。

面对历史系统的问题，密九令正好就是这么一款产品，能够很好的兼容历史系统，实现单点登录。对于历史系统完全是零改造，只需要在密九令系统填写配置信息即可适配业务系统，提供单点登录服务。用户访问业务系统时，SSO 服务器获取对应业务系统的配置信息，将对应该业务系统的用户认证信息（用户名

/口令)取出,代理用户登录业务系统;登录成功后,用户可以访问业务系统。

考虑到现用的业务系统的身份认证复杂程度不一样,为了能够适配更多的业务系统,可以单独为某个业务系统开发一个适配的插件,提高密九令系统的适配性。

4.4. 针对应用服务器的准入控制

密九令系统不仅提供安全、统一、简单的身份认证,还提供一个增强认证网关,拦截所有访问业务系统的请求,并且检查请求是否有合法 cookie 值,有合法 cookie 值则请求反向代理到真正的业务系统,没有合法 cookie 值则返回 HTTP 重定向到 SSO 服务器进行安全身份认证。在业务系统原有的安全设置下,提供双层次的安全保障。

4.5. 网络结构的零改造

随着企事业应用系统的不断建设,企事业的网络环境也变的越发的复杂,很有可能一个小改动而导致牵一发动全身的局面,面对此种情况去部署单点登录系统,将会是一件费时、费力、高成本的事情。而密九令依托自己特有的增强认证网关服务器,在部署单点登录系统时,可以对现有的网络结构进行零改造,完全不用担心因网络问题带来的高成本、周期长、风险大、影响日常工作等问题。

4.6. 支持 RDP/SSH/VNC/TELNET 等远程应用协议

随着企事业业务系统不断扩建,要维护的服务器也会越来越多,运维人员也要面对记忆各种服务器随机生成的连接口令,增加了运维人员记录难度;连接远程服务器都是 C/S 模式,需要在个人的 PC 机上安装客户端、缓存远程服务器的帐号、口令才能连接远程服务器,造成了使用的不方便,PC 电脑人为的安全因素占比较大,增加了账号口令的泄漏风险。

面对以上问题,密九令的远程连接功能正好能够完美的解决,提供一个方便、安全的方式连接远程服务器。

1. 将传统的 C/S 连接方式改成了 B/S 方式,不在受连接客户端的限制,只需要个支持 HTML5 的浏览器(PC 浏览器、移动端浏览器均可)就能随时随地连接远程服务器。

-
2. 通过单点登录的方式连接远程服务器，避免运维人员记忆各种服务器的连接口令，减少工作难度，提升工作效率，统一身份认证，增加安全性。
 3. 连接的账号口令统一托管在 SSO 服务器，并且采用不同的密钥进行加密存储，保障数据的安全性。

4.7. 使用 OpenID 协议实现单点登录

传统的单点登录技术都是基于 cookie 方式共享实现的，此种方式有诸多的不便，例如要考虑的一个问题就是域名问题，因为同二级域名和不同二级域名的实现方式完全不一样，增加了 SSO 系统的开发复杂程度，提高了开发成本，部署时也可能需要对已有的网络结构做改造，增加了部署成本和复杂程度。当使用 IP 地址的方式访问业务系统时，单点登录功能有可能失效，如果共享的 cookie 被窃取时，将能访问所有的业务系统，不够安全，基于以上种种问题，传统的 cookie 共享实现方式已经不利于构建一个认证方便、简单、安全的统一身份认证平台。

面对诸多问题，使用 OpenID 协议实现单点登录，都能迎刃而解，从实现协议上提升密九令系统身份认证的安全性。每个业务系统登录时都需要去 SSO 服务器进行身份认证，并且业务系统也需要对 SSO 服务器下发的身份认证信息进行签名验证，保证身份认证信息的安全性，并且不存域名问题、IP 地址访问等限制，不用对现有的网络结构做改造，减少部署的成本和复杂度。OpenID 协议已经是一个非常成熟、健壮的统一身份认证协议，使用起来非常简便，为构建一个方便、简单、安全的统一身份认证平台奠定了基础。

4.8. 完善的数据保护

密九令非常注重数据存储的安全性，所以提供了完善的密钥派生机制来对敏感数据、系统的配置信息进行加密保护。例如：每个 OpenID 应用的签名密钥都采用不同的密钥进行加密存储，每个应用系统托管的账号、口令都采用 SSO 用户参与派生的密钥进行加密，防止数据库一些简单的插入操作就能获取到应用系统账号、口令的明文。

第五章 扩展应用

5.1 SM9 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。

5.2 IBC 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。

OLYM[®] 奥联