方案优势

符合公安部等保三级要求

方案所采用的产品都经过国密局认证，拥有自主知识产权。整体方案符合公安部公信安（2018）1606号文《党政机关事业单位和国有企业互联网电子邮件系统安全等级保护扩展要求》中的等保三级要求；

先进的国家SM9算法体系

方案采用国际主流的标识密码技术保护邮箱安全，可实现基于策略加解密、外域先加密发送、跨域加密互通，轻量级管理中心管理海量用户；综合使用SM9/SM3/SM4等算法，对邮件数据全程加密保护，支持强身份认证，整体解决了传统邮件身份认证、传输和存储三大核心问题；

易于部署和使用

适应多款主流邮件厂家的系统，无须改变用户现有使用习惯，用户使用方便快捷；提供了客户端、WEB端、基于策略等实现加密解密功能，适应各种应用场景。

成功案例

- 全国人大
- 全国政协
- 国务院办公厅
- 国家发展改革委
- 国家信息中心 STATE INFORMATION CENTER
- 国办应急办
- 四川省政府
- 云南省委
- 湖南省政府
- 广西壮族自治区政府
- 北京市安全局
- 大连市政府
- 中国人民银行 THE PEOPLE'S BANK OF CHINA
- 中国信息安全测评中心
- 国家电子政务外网管理中心安邮中心
- 国家信息安全技术研究中心
- 国家电力监管委员会
- 法人单位基础信息库
- 药品价格评审中心
- 投资项目在线审批监管平台
- 国家应对气候变化战略研究和国际合作中心

深圳奥联信息安全技术有限公司

地址：深圳市宝安区宝安大道好旺角商业裙楼四楼

电话：4007-188-177

网址：www.myibc.net

密9邮 OLYM·SM9·INSIDE

SM9 电子邮件安全解决方案

IBC

邮件风险

电子邮件由于其技术和协议原因，传输和存储过程均是明文，攻击邮箱系统已是APT攻击的最主要途径。近两年邮件泄密事件频发例如2106年美国总统竞选期间希拉里“邮件门”事件、欧洲最大电线电缆制造商德国莱尼集团4000万欧元邮件诈骗事件，2017年美国中央情报局（CIA）前雇员斯诺登邮件泄密事件等。

政策支持

近年来，国家发改委信息安全专项推出“基于标识密码技术的安全邮箱试点示范”、信安标委“安全电子邮件标准”制定、公信安《党政机关事业单位和国有企业互联网电子邮件系统安全专项整治行动方案》公信安《党政机关事业单位和国有企业互联网电子邮件系统安全等级保护扩展要求（试行）》《党政机关事业单位和国有企业互联网电子邮件系统迁移指南（试行）》等，都彰显了国家对电子邮件安全的高度重视。

核心模块

SM9标识密码机、标识管理平台、邮件加密机、加密邮件网关、ZDM解密服务器、专用邮件客户端。

解决方案

该方案基于标识密码(SM9)技术对电子邮件实现增强身份认证、传输加密、存储加密由邮件系统SM9邮件加密系统、专用邮件客户端组成，实现以下功能：

邮件加密存储

邮件客户端、服务器端所有邮件数据实现加密存储即使黑客攻破服务器，也只能拿到密文无法破解；

邮件加密传输

邮件正文和附件均先加密再传输，不怕窃听拦截和泄密；

安全客户端

专用客户端可实现本地存储加密；

增强客户身份认证

双因子机制，查看邮件必须输入私钥密码同时支持使用USBKey认证；

邮件内容防篡改

数字签名算法可确保邮件内容没有被篡改或伪造；

异常邮件探测

对异常邮件数据和口令破解等行为进行监测和报警。

