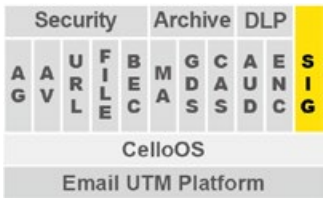
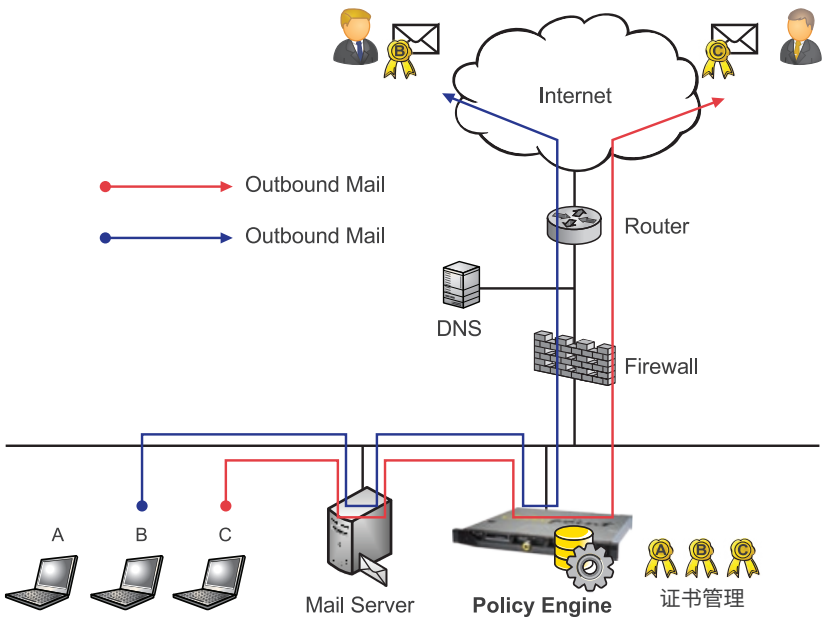
Prevent email forgery and ensure authentication as well as integrity of emails.

电子邮件数字签名 (SIG)

数字签名结合 Policy Engine，将所有符合策略的邮件主动添加数字签名，确保邮件数据的完整性 (Integrity) 与不可否认性 (Non-Repudiation)，并且借由网关端数字证书的统一管理，可简化管理人员维护数字证书与安装的过程，大幅提升数字签名的使用效率，并且强化组织待发邮件的风险管理。





解决邮件伪冒问题

电子邮件伪冒日益严重，Email 数字签名的采用对政府单位或所有需要证明电子邮件的不可否认性 (Non-Repudiation) 的单位都相当重要。但目前市面上数字签名因有数字证书安装等问题而导入不易，因此 Cellopoint 结合网关端的邮件策略引擎 (Policy Engine) 支持定义所有需要签名的账号皆自动在邮件发出时添加数字签名，不仅导入简易，而且节省管理员教育使用者的时间。

它采用匣道端 S/MIME 数字签名来达到防伪冒功能。如同正式签名，S/MIME 数字签名具有下列的安全性功能：

- **验证身份**：S/MIME 签名可用来确认发件人身份，验证该邮件确实为该发件人发出，并且证明该发件人个体的唯一性
- **邮件不可否认性**：S/MIME 签名是由发件人专属的私钥进行邮件签名，当收件者收到邮件进行验证，发件人无法否认曾经发出该封邮件
- **数据完整性**：S/MIME 数字签名所提供的另一项安全性服务是数据完整性。S/MIME 签名是针对电子邮件内容进行签名，用以保障数据的完整性。收件者收到签过名的电子邮件并验证后，即可确信所收到的电子邮件便是发件人当初签名传送的同一封邮件，并未在投递过程中遭到窜改。邮件一经签名，若在投递的过程中有任何修改，都会导致签名失效

解决问题

- 防止外发邮件伪冒
- 组织强制执行签名策略
- 确保邮件不可否认性
- 遵从数据隐私法规
- 保障传输安全
- 避免敏感机密外泄
- 遵从电子签名法

产品特色

- 符合业界签名标准
- 数字签名统一管理
- 最低总持有与维护成本
- 自动签名，管理无负担
- 用戶不需安装额外软件
- 更易整合现有 Email 环境

解决方案 / 执行动作	传统电子签名	Cellopoint S/MIME 网关端
申请数字证书	需指导每位用戶登入申请数字证书，管理者负担大	由管理者统一替每位用戶申请数字证书
安装发件人数字证书	需指导每位用戶登入进行数字证书安装，管理者负担大	由管理者安装发件人数字证书至任一台设备上，并将数字证书导出，上传至 Cellopoint 设备
设定邮件软件使用发件人数字证书	需指导每位用戶设定邮件软件使用发件人数字证书，管理者负担大	不需要
邮件加签名动作	需策略倡导要求每位使用者写完邮件后，必须点击邮件签名按钮，发件人可能因为疏忽而忘记添加签名	管理者统一在 Cellopoint 设备上设定邮件策略，每位发件人自动添加 S/MIME 签名，没有发件人可以规避的策略或规范空间
后续维护	当有新进人员或是有增加第三方人员时，需再指导人员申请数字证书、安装数字证书、设定邮件软件，并且提醒发件时，必须要加上邮件签名，管理者负担大	管理者只需将新进人员或是第三方人员的数字证书加入 Cellopoint 网关即可

规格表

SIG 型号	50, 100, 250	500, 1000, 2000	5000, 10K, 20K	Service Provider
每日处理邮件数量	5~25 万封	50~200 万封	500~2000 万封	2,000 万封以上
硬件性能 (可承载人数)	50 ~ 250	500 ~ 2,000	5,000 ~ 20,000	20,000 ~ Unlimited
Policy Engine	✓	✓	✓	✓
S/MIME 模式	✓	✓	✓	✓

※ 以上产品皆包含一年产品授权及标准保修，可依需求购买 1~N 年保修服务

※ 软件授权依电子邮件帐号数量计价

支持邮件系统

- Microsoft Exchange 2007/2010/2013/ 2016/Office 365/ Exchange Online
- Lotus Domino
- Novell GroupWise
- Sendmail, Qmail, Postfix
- Zimbra
- Coremail