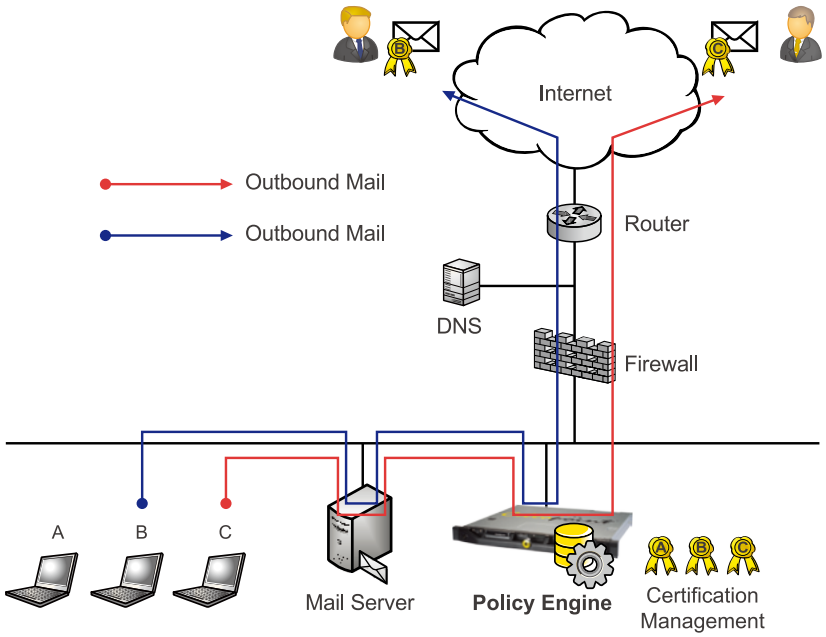
Prevent email forgery and ensure authentication as well as integrity of emails.

Email UTM

Digital Signature (SIG)

Cellopoint Digital Signature works with policy engine to automatically apply signature to specified email. Digital signature can ensure the integrity and non-repudiation of messages and it eases management effort by unifying certificate at the gateway level. As a whole, it enhances the usage of digital signature and improves organization risk management.



Either if is approving purchase orders or ensuring the legitimacy of a contract, the need of adopting a digital signature is critical for government, financial entities and other organizations to demonstrate authenticity. However, the installment of the certificate is complicated, and employees, careless or intentionally, avoid applying it.

Cellopoint utilizes the policy engine to automatically add digital signature to all the predefined accounts. This not only reduces the deployment effort, but also saves time to train and educate each user on the importance of applying the signature before sending an email.

Features

- Automatically apply digital signature, lower management burden
- Users do not need to add other plug-ins
- Easily integrate current email environment
- Follow industry certification standards
- Unify management of certification.
- Can import external master certification

Cellopoint
Secure Your Email

Advantages

Identity Authentication

Adding a digital signature simply means you apply your unique digital mark to the message. It demonstrates the identity of the sender is from a valid sender address.

Non-Repudiation

SIG utilizes your private key to apply the mark. When recipient receives a notification for authentication purpose, the sender cannot deny that the email was written by them.

Unify Management

Administrator can apply digital signature to all or just specific outbound email accounts (rules may vary depending on organization requirement). This reduces the risk of some users of not applying the certificate due to unawareness.

Trusted by desktop email clients

Cellopoint SIG is compatible with email applications such as Microsoft Outlook/Express, Mozilla Thunderbird, Apple Mail etc.

Integrity of messages

Recipient can verify the message by its signature, and be sure that the message received was not tampered or modified. Any modification of the mail through transmitting process will fail to pass through as a valid mail.

Encrypt Message

SIG can also be used as an encryption method to protect the email content in transmission. The recipient can be sure that the email was not tampered in the process and that is legitimate sent from the original author.

Master Certification

Cellopoint has the alternative of importing an external master certification and time stamp or choose Cellopoint to provide the certificate. Cellopoint certificates comply with Secure/ Multipurpose Internet Mail Extensions (S/MIME) standards.

Specifications

SIG Module	50, 100, 250	500, 1000, 2000	5000, 10K, 20K	Service Provider
Daily processing mails	50,000 ~ 250,000	500,000 ~ 2 Mil	5 Mil ~ 20 Mil	20 Mil
Authorized License	50 ~ 250	500 ~ 2,000	5,000 ~ 20,000	20,000 ~ Unlimited
Policy Engine	✓	✓	✓	✓
HTTPs method	✓	✓	✓	✓
S/MIME method	✓	✓	✓	✓
Warranty and Updates	1 Year Warranty and software upgrades (Can be extended to 2 – 5 years)			
Calculation of Accounts	SIG module is calculated by the number of email accounts, which includes email accounts and group accounts, but does not include alias.			

Benefits

- Organizations can enforce digital signature to all or specific employees
- Ensure the non-repudation of email
- Comply with regulations
- Ensure transmission of data
- Prevent sensitive data from leaking

Groupware and Email System supports

- Microsoft Exchange Series: 2003 / 2007 / 2010 / 2013 / Office 365
- IBM Lotus Domino
- Google Apps
- Novell GroupWise
- Sendmail, Qmail, Postfix
- Zimbra
- AWS SES

Cellopoint®
Secure Your Email