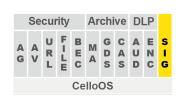


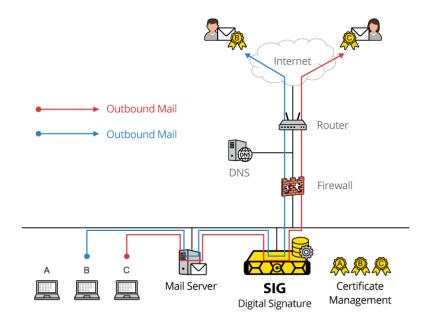


Prevent email forgery and ensures authentication as well as integrity of emails.

# **Digital Signature (SIG)**

Cellopoint's Digital Signature (SIG) integrates with a policy engine to proactively add digital signatures to all policy-compliant emails, ensuring the integrity and non-repudiation of outgoing emails. By managing certificates uniformly at the email gateway, it simplifies the maintenance and installation process for administrators, greatly enhancing the efficiency of digital signature usage. This solution helps organizations to prevent email spoofing and strengthen the risk management of outgoing emails, whether they use cloud services such as Microsoft 365, Exchange Online and Google Workspace, or on-premises platforms like Microsoft Exchange and Zimbra.





#### **Problem Solving**

- Prevents outgoing email spoofing
- Enforces mandatory signing policies
- Ensures email nonrepudiation
- Complies with data privacy regulations
- Ensures email transmission security
- Avoids sensitive data leakage
- Adheres to electronic signature laws

## SIG features at a glance

As email spoofing intensifies, adopting digital signatures is crucial for government agencies and any organization needing email non-repudiation. However, existing solutions often face implementation challenges like certificate installation. Cellopoint addresses this by integrating a policy engine at the gateway, which automatically adds digital signatures to required emails, easing deployment and saving administrators time by reducing the need for user training. Cellopoint SIG uses gateway-based S/MIME digital signatures to provide anti-spoofing functionality.

Cellopoint SIG offers the following features:

- **Identity Verification:** S/MIME signatures verify the sender's identity, confirming that the email came from the claimed sender.
- Non-repudiation: S/MIME signatures use the sender's private key for digital signing. Once verified by the recipient, the sender cannot deny having sent the email.
- Data Integrity: S/MIME digital signatures ensure that the received email is identical to the one sent by the sender and remains unaltered during transit. Any changes made after signing will invalidate the signature, indicating potential tampering.



Solutions Actions required	Traditional digital signatures	Cellopoint S/MIME digital signatures	
Certificate Application	Admins must guide each user to apply for certificates, which is burdensome.	Admins can apply for certificates on behalf of each user.	
Sender's Certificate Installation	Admins must guide each user through the certificate installation, which is burdensome.	Admins can install the senders' certificates on any device and then export and upload it to Cellopoint.	
Email Software Configuration for Sender's Certificate	Admins must guide each user in configuring their email software to use the sender's certificate, which is burdensome.	No need.	
Email Signing	Admins must enforce a policy requiring users to press the email signature button after composing.	Admins can configure S/MIME signatures to all users on Cellopoint, ensuring no sender can evade the policy.	
Ongoing Maintenance	When new or external personnel join, admins must guide them through certificate setup, email configuration, and signature reminders, which is burdensome.	Admins only need to add the certificates for new or external personnel to the Cellopoint gateway.	

## **Specifications**

SIG Models	50, 100, 250	500, 1000, 2000	5000, 10K, 20K	Service Provider
Daily Capacity	5~250k	500k~2Mil	5Mill~20Mil	Above 20 Mil
Active Email Users**	50 ~ 250	500 ~ 2k	5k ~ 20k	20,000+
Policy Engine	✓	✓	✓	✓
S/MIME	✓	✓	✓	✓

<sup>\*</sup>Flexible module licensing includes an initial fee for first-year license access, followed by maintenance fees.

#### **Features**

- Industry-standard digital signature compliance
- Centralized digital signature management
- Minimal total ownership and maintenance costs
- Hassle-free automated signature management
- No additional software installation required for users
- Easy integration with existing email environments

### **Supported Email Systems**

- Microsoft Exchange 2016
   / 2019 / 2022 / Microsoft
   365 / Exchange Online
- HCL Note
- Google Workspace
- Sendmail, Qmail, Postfix
- Zimbra

<sup>\*\*</sup>The number of licenses is according to the number of email accounts.

<sup>\*\*\*</sup>Cellopoint only provides software licenses; the appliance is not included.