SOLUTION BRIEF

Echoworx Integration With DigiCert

Making Certificate Encryption Easier through Auto-Generated S/MIME Credentials

ECHOWORX™

Key Benefits

- Echoworx Email Encryption seamlessly integrates with your DigiCert account to automatically generate trusted S/MIME certificates for employees; reducing IT workload.
- For organizations with high employee turnover that depend on S/MIME for email security, this automation eliminates manual steps during onboarding and reduces potential human error.
- All outbound encrypted emails and related notifications are signed using valid, trusted S/MIME credentials from the sender's corporate email address, ensuring secure and reliable communication.

1 2 3 4

Configure

Set up your DigiCert account. Create your certificate profile for REST API. Obtain your API key.

Setup

During onboarding, Echoworx will configure your tenant, profile, and set up your signing mode.

Enable

Echoworx activates S/MIME encryption in your console.

Test

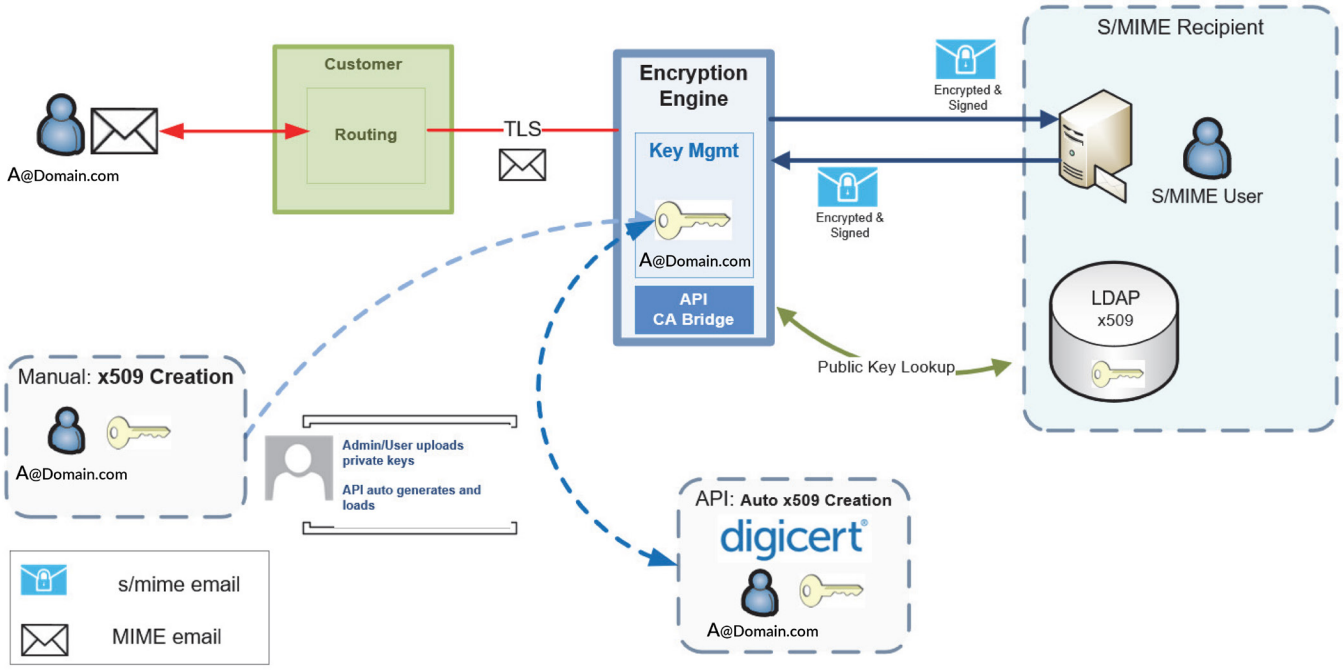
Validate your profile.

As digital transformation efforts progress, more and more digital assets have become mission critical. As this happens, the scope of what enterprises need to protect grows exponentially. Digital certificates are crucial for building trust across sectors. But digital certs are challenging to create and manage at the scale enterprises are now dealing with.

Using Echoworx's encrypted cloud service, an S/MIME message—signed or encrypted and signed—uses DigiCert's API to generate credentials for any sender without an existing private key. Credentials are created instantly, ensuring every email is signed by the sender; speeding things up, increasing use, and making management easier.

Integrated Solution

Echoworx provides automated S/MIME credential generation by integrating with DigiCert's REST API. When using the Echoworx Encrypted Mail Gateway (EMG) cloud service to send secure messages, EMG leverages DigiCert's API to create credentials for senders lacking a private key. This streamlines onboarding for organizations with high employee turnover using S/MIME for email security, reducing errors. All outbound encrypted emails and related notifications are authenticated by valid, trusted S/MIME credentials associated with the sender's corporate email address. Note: The email domain for the certificate generated must be owned by you and pre-validated by DigiCert.



DigiCert + Echoworx: Use Case Summary

- **Challenge**
  A major private banking and asset management group needed to automate certificate management for encryption platform users. The goal was to handle certificate issuing and renewing without manual intervention and integrate with an external PKI following common standards (e.g., RFC2797).
- **Solution**
  Implementing Echoworx's encrypted cloud service, the group used DigiCert's API to automate the generation of credentials for any sender, even those without an existing private key. This ensured efficient handling of every S/MIME message in real-time.
- **Result**
  The automated system instantly created credentials, ensuring every email was signed by the sender. This sped up communication, increased usage, simplified management, and ultimately enhanced the organization's security posture.