Seamlessly Secure Email Communications Across Your Enterprise

Deploy and administer Digital Certificates for S/MIME effortlessly

Who is DigiCert?

DigiCert is the premier provider of high assurance digital certificates, simplifying PKI-based security solutions for business of all sizes.

We're experts in encrypting sensitive data, ensuring secure communications, and providing identity authentication and customizable certificate management solutions.

- **2.0+ Billion** device certificates issued to date
- **89%** of Fortune 500 companies
- **97 of the world's 100** largest banks
- **93%** of encrypted global ecommerce transactions
- **28.9 billion** certificate status verification through OCSP daily

Good communication is at the heart of all successful organizations. But with cyberthreats on the rise, communicating and collaborating safely requires channels that are completely secure.

It's vital to have a stringent set of security measures in place, such as Secure/Multipurpose Internet Mail Extensions (S/MIME) protocol combined with digital certificates, for data encryption, message integrity and non-repudiation of message origin.

But, implementing and maintaining the Public Key Infrastructure (PKI) for the deployment of digital certificates can be complex and time-consuming. Even more so when the security for email needs to be constant and seamless across a dynamic organization.

The DigiCert® Trust Lifecycle Manager1 for S/MIME includes S/MIME key escrow service, certificate lifecycle management and the trusted DigiCert Certificate Authority (CA). It provides centralized email administration and recovery with secure key escrow, automated deployment of digital certificates, and flexible configuration and enrolment methods.

Your authorized users can be quickly set up to digitally sign and encrypt email communications across all corporate approved devices. Business applications are easily integrated with email security, making secure communications and user authentication a natural part of doing business.

And as you will be using a proven, scalable platform, you can meet the demands of a growing organization without placing any extra strain on your IT department.

With the DigiCert® Trust Lifecycle Manager, organizations can:

Protect personal information and corporate data with minimal cost and effort

- Protect personal information and corporate data with minimal cost and effort
- Gain complete visibility and control with centralized administration and recovery
- Easily manage compliance and IT changes with automated deployment
- Provide an exceptional end-user experience with seamless integration
- Instill trust in employees, customers and partners with user authentication
- Free IT teams to focus on other security issues

Secure email — your way

DigiCert® Trust Lifecycle Manager for S/MIME is highly configurable and maximum on flexibility. You have options of completely cloud-based deployment for simplicity, on-premises deployment to meet corporate security policies, or hybrid deployments for those who want to mix and match.

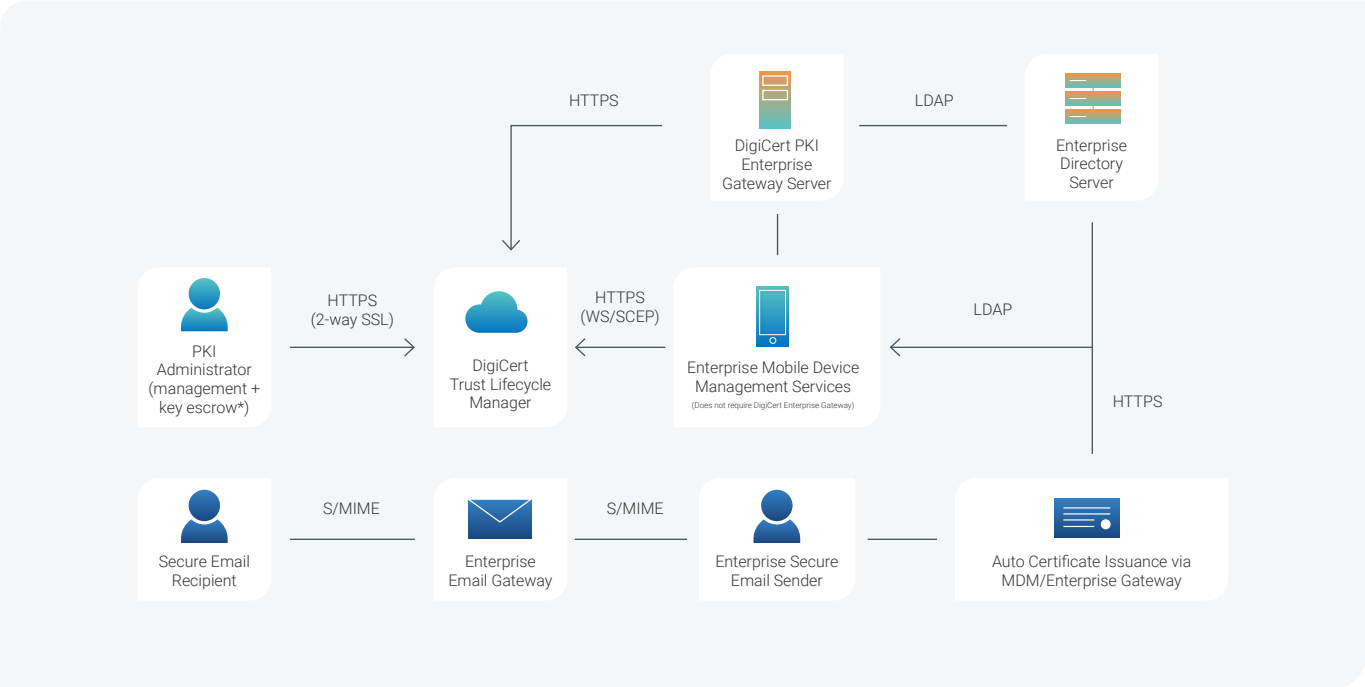
You can also choose from a range of enrollment and approval methods to match the exact needs of your organization. So, here are the three major steps to secure email, loaded with options:

1. **Perform centralized administration and email recovery with secure key escrow that's either:**
   - Cloud-based
   - Two-part recovery
   - On-premise with local Active Directory (AD) or HSM, Oracle, SQL server
   - Same key pair on all the end-user devices

2. **Choose an enrollment method and certificate profile that meet your needs:**
   - PKI client
   - Self-support portal
   - OS/browser enrollment
   - Mobile Device Management (MDM) web services

3. **Deploy a preconfigured workflow:**
   - Automated via PKI client with gateway and AD authentication
   - Automated via passcode
   - Automated via MDM service

PKI secure email for enterprise



Summary of benefits and features

Seamless integration with business applications

Integrates with Enterprise Device Management (EDM) and Mobile Device Management (MDM) applications, with Web Services and Simple Certificate Enrollment Protocol (SCEP).

Fast deployment

Over 30 pre-packaged certificate profiles for common applications such as VPNs, 802.11x WIFI, Web Services, Secure S/MIME email, Adobe® and Microsoft® applications included.

Automatic deployment of certificates to domain-joined machines via Windows Group Policy Object (GPO), with Active Directory (AD) integrations, or Light Directory Active Directory (LDAP).

Compliance with corporate security policies

Multiple enrollment methods available, including via: PKI client software (auto-enrollment), self-support portal, operating system/browser based and Mobile Device Management (MDM) Web services.

Cost-effective with maximum scalability

Top-of-the-line PKI infrastructure with dedicated multi-million dollar investments in Research & Development, maintenance, security and compliance.

Significant reduction in costs and management burden versus implementing and securing your own PKI environment. Proven capabilities to scale and process high-volume certificate requests quickly.

Industry-leading security

Powered by the same PKI technology as DigiCert's military-grade PKI and Network Operations Centers. Backed with 24x7x365 monitoring, management, and escalation support across the globe with full disaster recovery.

World-class professional and support services

DigiCert Professional and Support Services are available to help you throughout the solution lifecycle, from planning and implementation, to maintaining an in-house, full-scale support infrastructure.

Find out more

DigiCert provides enterprise-class SSL, PKI and IoT security solutions for some of the world's biggest organizations–providing peace of mind and keeping them and their data secure at all times.

To learn more about our managed PKI solutions, visit: www.digicert.com/mpki, call 1.801.701.9600 or email support@digicert.com