Sectigo Mobile Certificate Manager

In an expanding ecosystem that includes mobile devices and users bringing their own devices (BYOD), enterprises looking to prevent access from unauthorized users, applications and devices often use a "Zero Trust" model where trust is never granted implicitly and must be continually evaluated. The best in class approach is to use certificates for S/MIME, Wi-Fi, VPN, and browser client authentication. However, it is difficult to deploy certificates and keys (in the case of encryption), across the many devices that access enterprise assets, including email.

That is why security teams need a certificate management solution that can:

Issue certificates and keys to all mobile devices with or without an MDM, within or outside the enterprise.

Automatically renew certificates due to expiry, changes in certificate subject name, or cryptographic strength, so that device use is never disrupted.

Improve visibility using a single pane of glass, alleviating the headache of multiple key management portals, across multiple MDM and cloud vendors. This is important when a set of devices (or the certificate cryptography itself) is compromised.

Sectigo can help

With Sectigo Mobile Certificate Manager (MCM), you can issue and manage certificates and keys across iOS, Android and Chrome OS (Chromebooks) devices without user intervention. Sectigo supports all certificate types and is interoperable with all leading devices, operating systems, and MDM vendors.

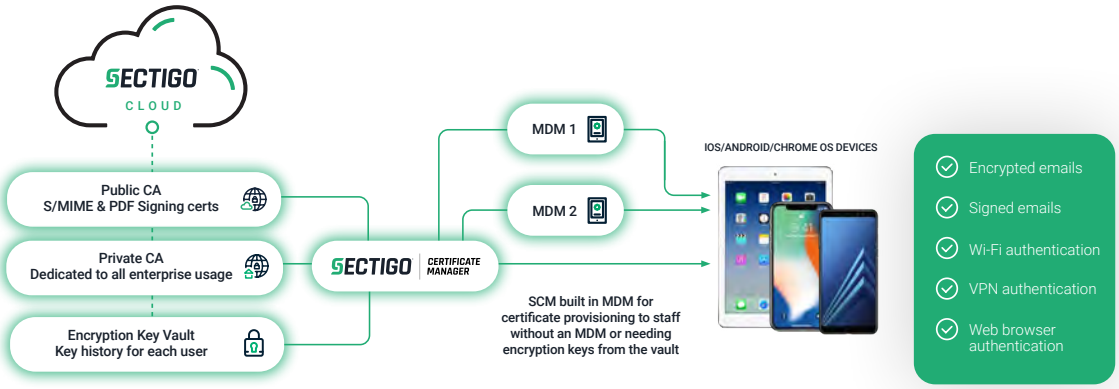
SECTIGO

Sectigo Mobile Certificate Manager (MCM) enables your security team to store and manage certificates on mobile devices using Sectigo Key Vault while also benefitting from:

- **Zero-Touch Distribution of Keys Across Devices**
  S/MIME requires that the same keys are distributed across multiple devices used for email. Sectigo MCM distributes entire encryption key history stored in Sectigo Key Vault to multiple mobile devices, so you can decrypt emails which used older keys on every device.
- **Zero-Touch Issuance of Keys for Wi-Fi, VPN, and Client Authentication**
  Sectigo MCM can can issue certificates at scale for Wi-Fi, VPN access and client authentication.
- **Automated Certificate Lifecycle Management**
  With Sectigo MCM you don't have to manually issue, revoke/replace, or renew certificates. All certificate operations are automated and can be done using a single platform, including where possible provisioning the application to use the certificate.
- **Passwordless Authentication on Mobile Devices**
  In order to implement Trusted Endpoints, certificates can replace one-time passwords (OTP) to authenticate both the user and the device, which simplifies the employee's experience.
- **Scalable Certificate Issuance**
  Whether your mobile users number in the dozens, hundreds, or thousands, Sectigo MCM lets you issue certificates in an automated manner, with or without an MDM. This is particularly useful if you have an MDM, but have employees that are contractors from other companies, and unable to install an MDM onto their devices.
- **Zero Trust assurance at the device level**
  Certificates are issued to each mobile devices ensuring only valid users and devices can connect to networks over the email sever, Wi-Fi, or VPN, or can access a website or cloud application. Where the hardware permits, Sectigo will install the certificate private key in such a way it cannot be extracted from the device.
- **Enhanced Visibility and Reporting**
  Sectigo MCM lets you view the status of the certificates in use through a single platform, enabling you to see expiration dates and cryptographic strength while eliminating service disruptions for both public and private certificates.

With Sectigo, you can enforce cryptographic strength, maintain compliance, and future-proof your business while minimizing costs. Sectigo Certificate Manager can also be used to automate issuance and lifecycle management of all other certificates throughout your organization, across a wide variety of use cases that require digital signing, authentication, and encryption.

Sectigo Mobile Certificate Manager (MCM)



About Sectigo

Sectigo is a leading cybersecurity provider of digital identity solutions, including TLS / SSL certificates, DevOps, IoT, and enterprise-grade PKI management, as well as multi-layered web security. As the world's largest commercial Certificate Authority with more than 700,000 customers and over 20 years of experience in online trust, Sectigo partners with organizations of all sizes to deliver automated public and private PKI solutions for securing webservers, user access, connected devices, and applications. Recognized for its award-winning innovation and best-in-class global customer support, Sectigo has the proven performance needed to secure the digital landscape of today and tomorrow. For more information, visit www.sectigo.com and follow @SectigoHQ.

SECTIGO