Device Management

PKI certificates allow multiple devices to securely access your network, protecting your systems. At the same time, the networks authenticate the devices. With PKI Platform, you can easily manage certificate deployment for over 20,000 company-owned devices and 30,000 BYOD devices.

Secure Devices - Use Case 1

1. Register with MDM
2. Enroll user for certificate
3. User identity confirmed
4. Access configured based on user role
5. Certificate issued
6. Delivers certificate
Secure Devices - Use Case 2

1. Register with MDM
2. Enroll user for certificate
3. User identity confirmed
4. Access configured based on user role
5. Certificate issued
6. Delivers certificate

Secure Devices - Use Case 3

1. Register with MDM
2. Enroll user for certificate
3. User identity confirmed
4. Access configured based on user role
5. Certificate issued
6. Delivers certificate

Auto-enrollment server retrieves certificate from PKI Platform and pushes certificate to Windows desktops / laptops with installation instructions.
Secure Devices - Use Case 4

1. All users download PKI Client for non-iOS devices through webpage and enroll for certificate.

2. User identity confirmed.

3. Access configured based on user role.

4. Unique enrollment code returned from MPKI Service and provided on webpage.

5. PKI Client or iOS auto-installs certificate.

Webpage → DigiCert PKI Platform → LDAP/Active Directory → PKI Client → Mobile devices, Windows Computers & iOS.