Entrust PKI Integration with Microsoft Intune

Entrust has the PKI expertise to help organizations get to where they want to go. With our comprehensive policy implementation and uniquely flexible and easily scalable PKI, you can establish and manage all of your use cases simultaneously – drastically increasing the speed of new application deployment without introducing risk. With Microsoft Intune, organizations can easily manage all of their mobile devices and applications, seamlessly enabling enterprise mobility.
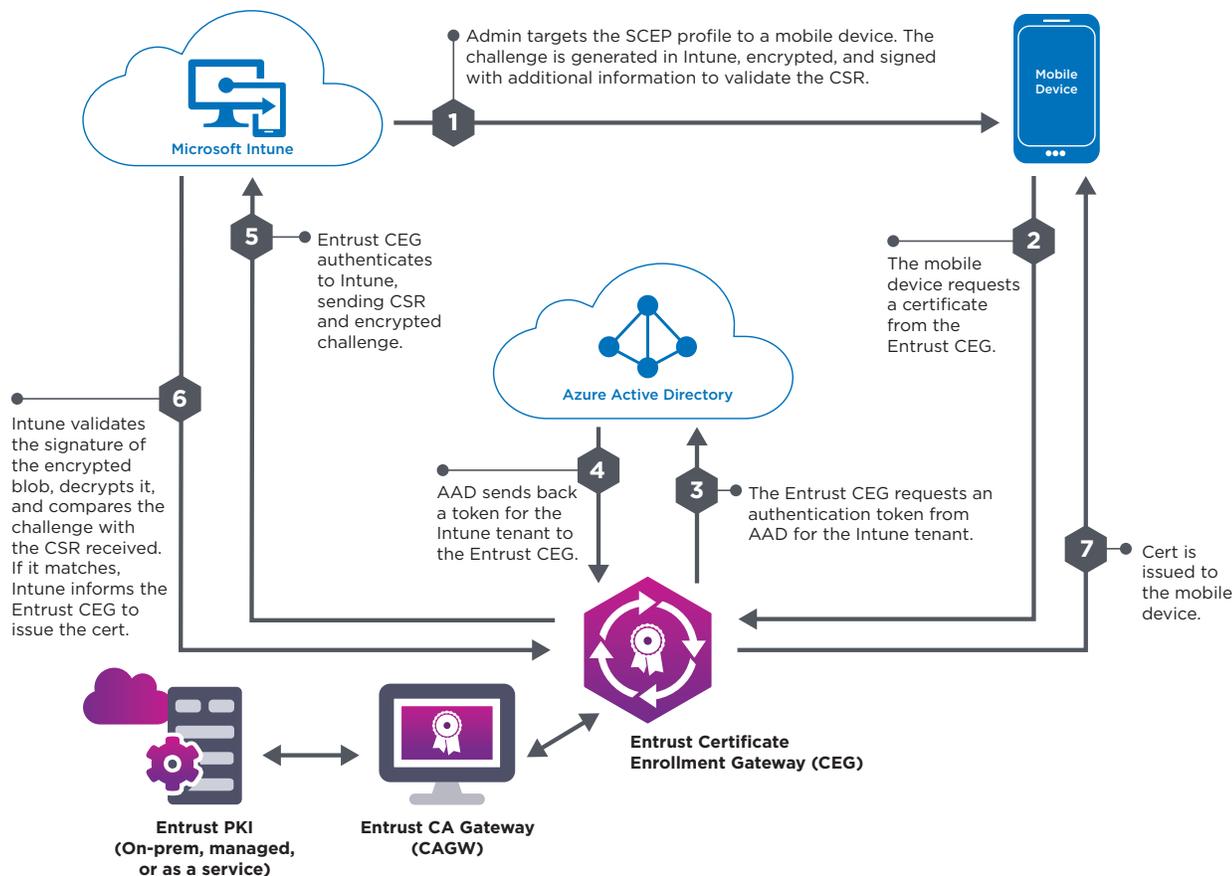
The combination of Entrust PKI - on premises, managed, or PKI as a Service - and Certificate Enrollment Gateway (CEG), with Microsoft Intune allows customers to leverage their PKI environments seamlessly with their enterprise IT management platform. The Certificate Enrollment Gateway provides a modular enrollment service, that when coupled with flexible and extensible PKIs allows devices of any kind to be enrolled securely with extended key and certificate parameters to support advanced identification, authentication, and authorization schemes.

BENEFITS

• High assurance certificate-based credentials for Intune deployments

• Leverage your enterprise certificate authority for managing Intune devices

• Integrates with Entrust PKI - on premises, managed, or PKI as a Service

• Full customizable certificate policy and definition allow for robust and extended use cases

• Rapid deployment

• Secure communications/ secure tunnel/VPN

• Crypto policy and algorithm management (data protection, encryption)
   - Different profiles for different devices – ECC vs RSA (key lengths)

   - Rotation policies

• Support for automatic revocation via Intune

Learn more about our PKI solutions at entrust.com

Entrust PKI Integration with Microsoft Intune

Microsoft Intune

1 Admin targets the SCEP profile to a mobile device. The challenge is generated in Intune, encrypted, and signed with additional information to validate the CSR.

Mobile Device

5 Entrust CEG authenticates to Intune, sending CSR and encrypted challenge.

Azure Active Directory

2 The mobile device requests a certificate from the Entrust CEG.

6 Intune validates the signature of the encrypted blob, decrypts it, and compares the challenge with the CSR received. If it matches, Intune informs the Entrust CEG to issue the cert.

4 AAD sends back a token for the Intune tenant to the Entrust CEG.

3 The Entrust CEG requests an authentication token from AAD for the Intune tenant.

7 Cert is issued to the mobile device.

Entrust Certificate Enrollment Gateway (CEG)

Entrust PKI (On-prem, managed, or as a service)

Entrust CA Gateway (CAGW)

The secure enrollment ensures no tampering occurs at any point in the certificate issuance. Organizations can issue certificates via Entrust to provide seamless authentication to applications and on-premises resources, creating a user-friendly, flexible, and cost-effective experience. All in addition to certificate-based authentication.

Key Capabilities

- Ensures secure delivery of keys and certificates to devices
- Leverages industry-standard SCEP protocol for maximum device interoperability
- Full credential lifecycle management through Entrust PKI
- Certificate publishing and validation services allow for real-time revocation checking

Learn more at
entrust.com

ENTRUST

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com