Using certificates and Public Key Infrastructure (PKI) to improve device security is a growing need in our increasingly connected world. As each device connects, a new attack vector becomes present, which hackers can and will exploit. Properly issuing, provisioning, and using certificates on devices will mitigate many of the risks introduced with connected devices.

An *improperly* implemented PKI solution offers little protection to safeguard your systems from the risk it is intended to mitigate. Given the critical nature of defending devices and networks from these new attack vectors, it is important to choose a partner focused on PKI.

Protecting issuing roots, publishing certificate revocation (CRL and OCSP), and maintaining a certificate server are a few challenges, among others, that can be solved by choosing DigiCert as your partner in PKI.
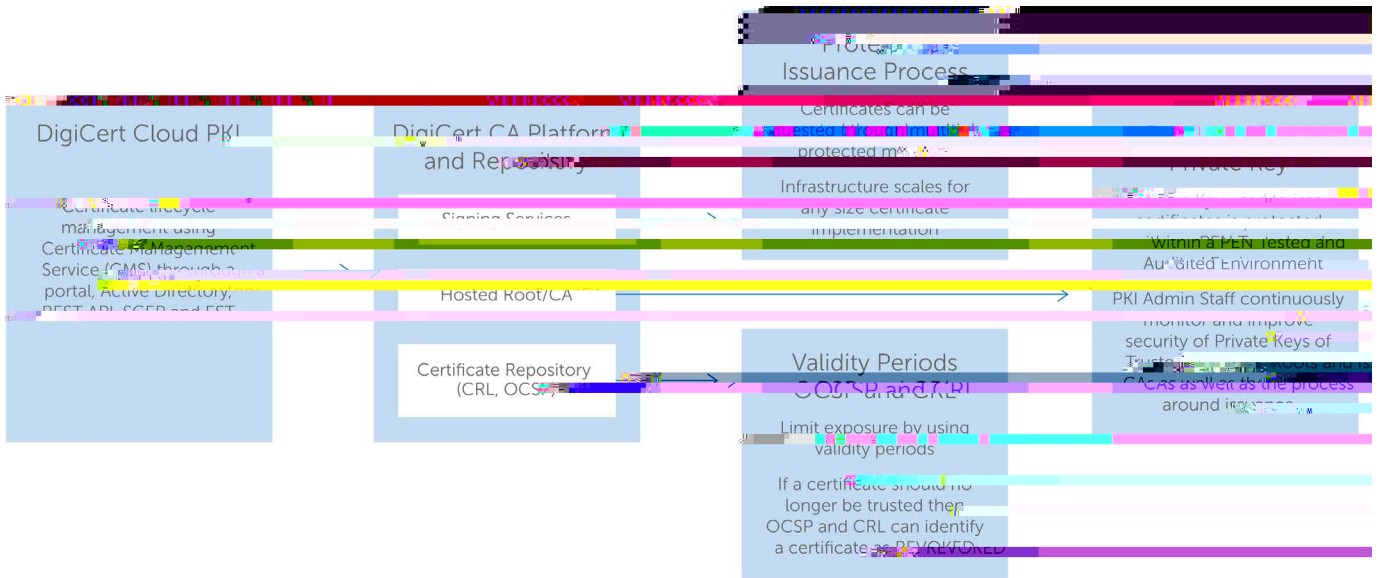
The following diagram shows the DigiCert Cloud PKI service and an example of the process of how a certificate can be requested and sent to a device.

IOT DEVICE CERTIFICATE ISSUANCE

The DigiCert Cloud PKI service provides a secure and stable infrastructure for you to confidently move your PKI implementation ahead.

DIGICERT CLOUD PKI

Work with our professionals and gain peace of mind that you are approaching device security in the right way, following best practices, and are always up-to-date with industry standards.

With an expert team who has a focus on securing IoT devices using PKI solutions, DigiCert will be a reliable partner in creating a custom solution that fits the needs of your organization.

We can architect a solution for your business. To talk to one of our PKI experts call 1.801.701.9642 or email healthcareiot@digicert.com.

di