DigiCert Private PKI

Organizations requiring encryption for internal systems need an Internal CA to issue their private SSL certificates. However, designing, developing, implementing, and maintaining the necessary supporting systems of your own private PKI can be a complicated, costly, and time-consuming feat.

Using the DigiCert Private PKI Solution allows you to request and manage internal certificates with ease, either through the account user interface or API. DigiCert offers both cloud and on-prem PKI solutions, as well as hybrid solutions, to meet specific needs. Choosing our hosted PKI solution affords many advantages, most importantly that you can control all facets of your private PKI without any of the maintenance headaches. See the below use-case:

PKI IMPLEMENTATION

Private SSL certificates are issued off a private, dedicated intermediate and root certificate. Unfortunately, securing your own root and intermediate can get very expensive. Some of the costs of PKI set up include:

- Hardware, software, and licensing
- PKI expertise
- Training
- Certificate Policy (CP)/Certificate Practice Statement (CPS)
- Auditing against Certificate Policy
- Vulnerability testing

With the DigiCert Private PKI solution, we will create your root and secure it at a level commensurate with public trust anchors, while allowing you oversight of your intermediate, its properties, what types of certificates it can issue, and the names on those certificates.

CUSTOM CERTIFICATE PROFILES

Once the private PKI is set up, you need to create your certificate profiles, also known as templates, to define what goes into the certificates you want to issue. However, creating and maintaining your own certificate can result in incorrect or missing extended key usages (EKUs) and certificate attributes, which can cause a lot of future grief.

With DigiCert Private PKI, you don't ever have to worry about mistakes in the certificate profile. Our team of experts will advise on what certificate profiles would be ideal for your organization, or you can use one of our turnkey private products that are immediately ready for use and match the most common use-cases we've dealt with.

USER AND ACCESS CONTROL

DigiCert Private PKI integrates with our enterprise-grade certificate lifecycle management platform, which provides refined and enhanced role-based permissions, account access, and audit logs for continuous monitoring. Because RA services are built-in to CertCentral, you don't need to wait for verification of your user requests, and you can perform approvals and control permission management in one location, allowing you to have valuable insight into how your PKI is being used, as well as the flexibility to grant appropriate access and permissions.

CERTIFICATE ISSUANCE

PKI implemented incorrectly is as good as no PKI at all. To maintain proper control and eliminate potential threats or vulnerabilities, you must constantly evaluate your certificate issuance process. But, in updating certificate profiles to align with industry standards and securely storing CA files, as well as public and private key exchanges, there are things that can go wrong or become obsolete.

Our CA software is already configured to handle this process, so all your certificates are issued within seconds without the threat of downtime or server outages. DigiCert Private PKI ensures your certificate issuance is faster, more efficient, and completely secure.

REVOCATION INFRASTRUCTURE

If you are a globally dispersed enterprise, it can take a significant amount of work to deploy modern revocation infrastructure. CRLs are difficult to maintain and a challenge to scale appropriately for an expanding PKI.

DigiCert private PKI offers two revocation mechanisms: CRL and OCSP. Both revocation services are globally distributed by our CDNs and managed automatically.

CERTIFICATE MANAGEMENT PLATFORM

After a certificate is issued with an internal PKI, there will be a record of it, but it will not necessarily send you reissue, expiration, or revocation notifications by default. And most likely, a certificate will require some ongoing management during its lifetime. For example, you may need to reissue a certificate because the private key was lost during a server outage, revoke a certificate because an admin left the company, or redownload a certificate because it needs to be installed on another machine.

Because our private PKI solution is integrated with CertCentral, you have the customized workflows and interface management to handle all stages of a certificate's lifecycle. CertCentral assists with core security infrastructure asset tracking: when you receive an expiration notification, you can escalate expirations so that the right personnel are notified at the right time; when it's time to renew, the metadata from the initial issuance is carried over, saving you time and energy; when something goes wrong in your account, you can receive automatic notifications with details around the events.

WHY CHOOSE DIGICERT

Effective PKI is more than simply implementing CA software—it requires constant diligence, adherence to industry standards, developing storage, data backup, and certificate management policies. DigiCert Private PKI lets enterprises enjoy the advantages of private SSL certificates, along with the management benefits of comprehensive administrative tools and the expertise of an award-winning CA, all without the hassle of setting up and maintaining your own PKI.

Want to talk more about the DigiCert Private PKI solution? Call 1.855.800.3444 or contact sales@digicert.com for further information.

digicert®