

DigiCert hybrid PKI for European sovereignty



Two factors have combined to make hybrid PKI the best solution for many organizations.

First: Certificate lifetimes are shrinking fast, reaching 47 days by March 2029. Because manual processes can't keep up with this lifecycle period, automation will soon be a necessity.



Second: European organizations need stronger control over where private keys, certificate authorities, and issuing software reside, keeping them on their own infrastructure and under their own policies.



European regulations are raising the bar on both fronts at once. NIS2 and DORA tighten operational resilience and incident-reporting requirements, penalizing outages and undocumented recovery processes, while eIDAS 2.0 and national data-residency rules require that organizations prove real control over their cryptographic infrastructure, not just rely on contractual assurances. A hybrid model is the only way to satisfy both sets of demands without a manual operations team standing behind it.

DigiCert's Hybrid PKI is designed to address both challenges for you. Automation runs from the DigiCert cloud control plane, which orchestrates certificate policy and isolated renewal scheduling, so renewals never lapse but other components of the lifecycle stay inside your security organization. Your root and issuing CAs, private keys, and hardware security module (HSM) remain entirely within your own environment, under your own control, policies, and infrastructure.

How the hybrid model works

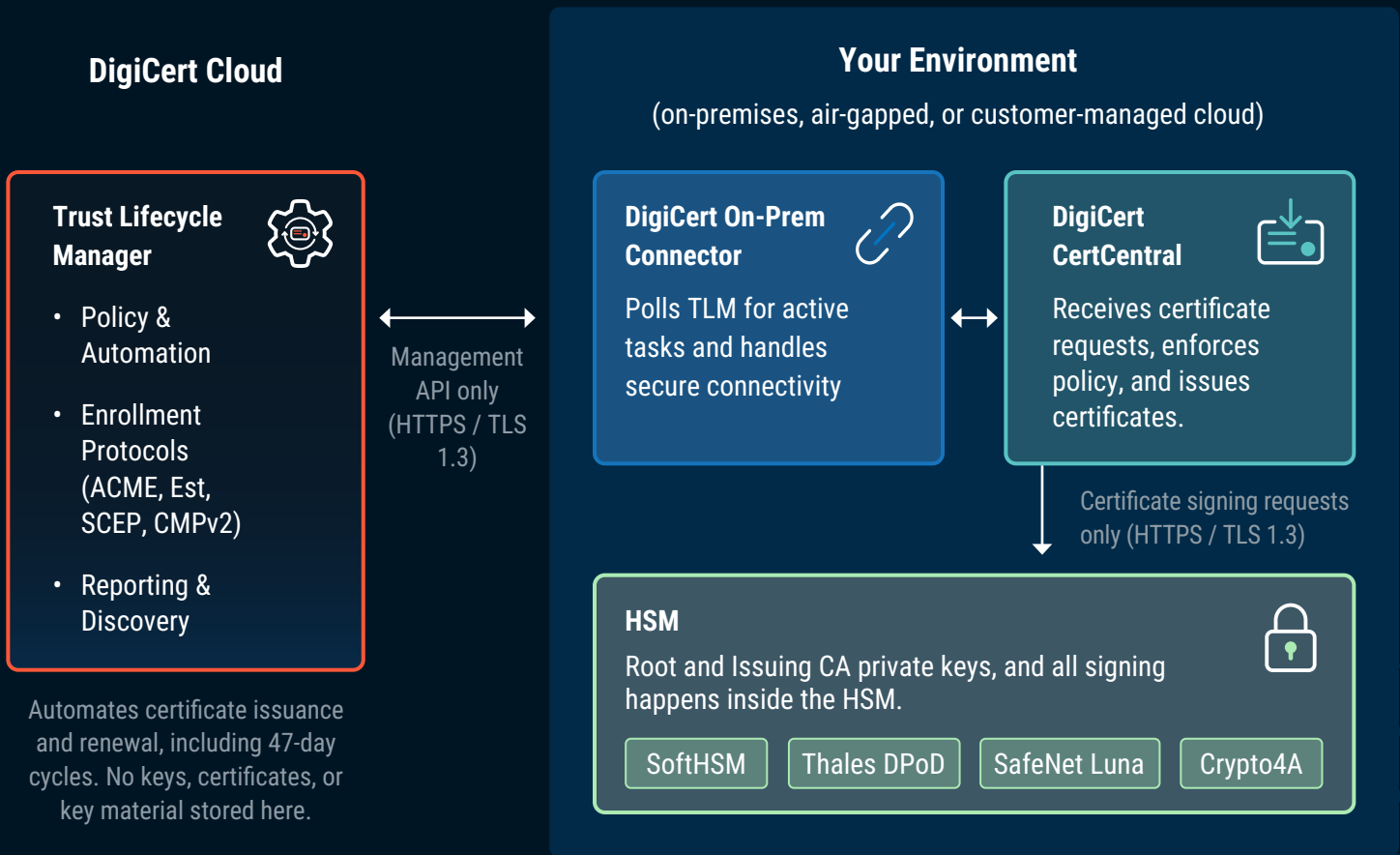
The DigiCert cloud control plane orchestrates certificate policy, issuance workflows, and renewal automation—the component that must keep pace with 47-day lifetimes.

Your root and issuing CAs, private keys, and HSM never leave your environment. They stay on your infrastructure and under your policies.

Certificates are issued and renewed automatically on schedule, without your keys or CAs ever transiting through the DigiCert cloud.

The DigiCert cloud control plane runs from European data centers in the Netherlands and Switzerland, ensuring both your keys and the control plane remain resident within the EU or CH.

Deployment options built for your infrastructure and sovereignty needs



End-to-end key sovereignty with DigiCert hybrid PKI



Maintain Key Sovereignty and certificate issuance management



Leverage your own secure Hardware Security Modules (HSMs)



Gain centralized on-premise CA visibility and full control of services



Eliminate latency with CA services hosted in your environment

DigiCert fully on-premises vs. DigiCert hybrid PKI

	DigiCert fully on-premises PKI	DigiCert hybrid PKI
Key & CA custody	Fully in your control, but you own all the infrastructure	Root/issuing CA, private keys, and HSM stay in your environment
Renewal automation	Manual, dependent on internal tooling	Automated from DigiCert's cloud control plane
Latency & availability	Local issuance, no external dependency	CA services run in your environment, no added latency
Operational overhead	High: you manage everything	Low: DigiCert manages orchestration, while you retain only the PKI components that must stay under your control for regulatory and data-sovereignty reasons

Is hybrid PKI the right fit for your organization?

Backed by over 20 years as a publicly trusted, WebTrust-audited root CA.

- You operate in the EU or serve EU customers under NIS2, DORA, or eIDAS 2.0 obligations
- You currently run PKI entirely on-premises and are outgrowing manual renewal processes ahead of the 47-day certificate lifetime
- You've evaluated a fully cloud PKI vendor but can't get comfortable ceding CA and key custody outside your environment
- You need to demonstrate to auditors and regulators demonstrable control over cryptographic infrastructure, not just contractual assurances

European QTSP: Audits and Certifications



Netherlands Qualified
Trust Services Provider



Belgium Qualified
Trust Services Provider



Trust Service Provider
for Kloverheid



PKI Provider for European Industry Standards



Ready to modernize your PKI while preserving key and data sovereignty? Contact your DigiCert team to scope a hybrid deployment.

Learn more about
[European Qualified Certificates](#)