**DigiCert Keys**

* Root Keys are stored offline in tamper-resistant hardware tokens locked in safes.
* All signing keys are stored in FIPS 140-2 certified Hardware Security Modules (HSMs)
* The HSMs require multiple trusted individuals to activate and operate.
* The HSMs are stored in secure data centers requiring biometric access, and physical access to the cabinets housing them requires multiple trusted individuals.
* There are additional layers of physical security (proprietary - can’t be shared) protecting the HSMs that are.
* The HSMs are only "visible" to trusted "CA" servers.
* The trusted "CA" servers are only accessible by "Application" servers.
* The Application servers are not publicly accessible either.

**Internal Processes**

* DigiCert validation staff do not have administrative access to their PCs.
* IT/Security staff run hardened configs on their own laptops/PCs.
* Access to all servers is extensively monitored so that any application layer breach can be detected immediately.
* Of course, no remote SSH or RDP access is publicly allowed.
* All systems are configured to syslog to a central host.
* Syslog reports are sent out (and reviewed) at 15 minute intervals.
* We've taken pains to make the server environment as “noisy” as possible so that it would be extremely difficult to gain a foothold on one of our servers without being detected within hours if it ever does happen.

**Web Applications and Servers**

* Web application servers are hardened, configured to run in chroot jails, with unneeded tools and even parts of the programming languages disabled (blacklisted functionality)
* Web applications are syslog verbose so that all suspicious and other error conditions are quickly detected in syslog reviews.
* Web applications use two layers of protection from SQL Injection: prepared statements + a custom API that also scans each data input for suspicious content so that it can syslog all its suspicions (instead of just rejecting them silently)
* Web application servers have special outbound firewall rules, limited to needed communications with other servers only. We’ve made use of the -m owner iptables module to restrict the apache user to only the packets it needs to send. All other packets result in noisy syslog DROP notifications that are very-frequently-monitored syslog reports.
* Access to our internal order management web application requires an allowed IP address, a client SSL certificate only DigiCert could issue with field-level matching of certain fields required, a valid username/password, and a one-time-password.
* Apache web application servers are located behind Nginx caching proxy servers.
* File alteration monitoring is in place on all servers, reviewed daily.
* Various booby traps exist which immediately notify security administrators (including CTO) via text messages if ever tripped.
* Applications syslog all suspicious conditions (detection of probing such as SQL injection typically results in firewall response)
* Web applications are coded securely against malicious inputs - with multiple layers of filtering against SQL injection, XSS, and other malicious input.

**Scanning and Other Protections**

* This should go without saying, but all passwords stored in the database are encrypted with a SECURE, SALTED hash algorithm.
* Publicly visible web servers are regularly scanned for vulnerabilities by 3rd party PCI scanning services.
* We run QualysGuard in the office network to regularly scan staff computers.
* We use Aruba controllers for wireless rogue detection (including triangulation), in addition to a guest wireless segment which is completely isolated from the wired office network.
* Office wired ports run in "protected vlan" so that protected ports can't see each other (in order to limit what an attacker with a foothold would be able to scan)
* Anti-virus is installed on all Windows systems.
* We scan ourselves with 3rd party web vulnerability scanners to look for holes.
* We screen our staff with background checks and reference checks and renew background checks regularly
* We hold staff training meetings to teach security principles and our e-Policies.
* We do not employ any fully automated systems.
* We maintain a list of the Alexa top 500 into an internal restricted names list: if any request ever makes it to the CA core for one of those domain names, it will of course refuse to issue the request, but it will also syslog distress signals that will be immediately repeated as text messages to the IT/Security team's phones.

**Additional Differentiators in Process**

* We've built an IP reputation tracking system based on feeds like DSHIELDS.
* We're constantly working on security enhancements – the effort never stops – examples of current projects are:
  + working down the SANS Top 20 list, prioritizing projects based on what will most improve our security stance in shortest amount of time.
  + building new network forensics logger servers to install in the office network as well as between our application servers and our CA core.