

TLS/SSL Professional Services by DigiCert

At-a-glance

TLS/SSL Professional Services by DigiCert provides superior certificate management consulting for businesses worldwide. Receive in-depth training and guidance on implementation and management of your TLS/SSL solutions from the world's largest Certificate Authority—DigiCert.

Unmatched experience

With an average of over 20 years of technical experience, our professional services engineers have worked with all types of organizations, from small businesses to Fortune 500 companies, and facilitated secure communications across public and private ecosystems on a global scale.

Using a proven framework and best practice approach, our consultants customize each engagement to help you efficiently design, architect, develop, and deploy your products and services. Many consultants hold industry certifications (such as CISSP or Security+) and have managed complex security and infrastructure projects.

Overview of services

Our range of services have been designed by our engineers with your organization, process and people in mind. From supporting the implementation of key DigiCert CertCentral® TLS Manager capabilities, to sharing our industry expertise with your team, we are here to help at every stage of your journey with us.

Key Benefits

- Solutions tailored to address your business needs
- Fast rollout and implementation
- Subject matter experts and a point of contact to assist every step of the way
- Backed by the world's leading provider of TLS/SSL, PKI, and IoT solutions
- Solutions from the most scalable and reliable TLS/SSL infrastructure

Our services include:

- TLS Health Check
- CertCentral API consulting
- Certificate Discovery
- Certificate Automation
- Training & Workshops

TLS/SSL Health Check

The TLS/SSL Health Check includes a scan of your internal and/or external websites, report creation and review. We will scan your internal and/or public websites to detect TLS/SSL certificate risks and vulnerabilities including:

- Potential TLS/SSL certificate security risks
 - Expired/revoked certificates
 - Untrusted roots
 - Missing/incomplete trust chain
 - Weak keys and hashing algorithms
- TLS/SSL server vulnerabilities
 - Heartbleed
 - Poodle
 - FREAK
 - BEAST
 - CRIME

After completing the health check, we will create a detailed report listing any issues discovered and present the report—along with our recommendations.

CertCentral API Consulting

The DigiCert Services API is a powerful tool that allows you to automate typical certificate processes to save time and streamline certificate management. We provide training and guidance to help you set up a custom integration. This includes knowledge transfer about the API and assistance with the configuration of your CertCentral account. The DigiCert Services API uses modern RESTful conventions and allows you to:

- Access all the features available in CertCentral without needing to log into the platform
- Customize and automate virtually any workflow within the certificate management platform
- Create your own version of the platform with your organization's branding
- Seamlessly integrate with your existing tools

CertCentral Discovery deployment

DigiCert CertCentral Discovery is a service enabling the detection and monitoring of TLS/SSL certificates installed across an entire environment regardless of the issuing Certificate Authority. Our service uses an advanced hybrid deployment model to give you complete, integrated control over your TLS/SSL certificates.

Discovery benefits

- Get a comprehensive view of the certificates in your networks
- Avoid unplanned outages due to certificate expiration
- Identify and remediate vulnerabilities and security issues

We will work with your network and security teams to successfully deploy CertCentral Discovery within your enterprise. This will usually include the following steps:

1. Planning workshop – Demonstrate a working solution in the Aberdeen Standard certificate environment.
2. Deploy discovery – DigiCert will work with the customer to deploy SSL sensors at strategic points in the customer's network. These sensors will scan for SSL certificates periodically, build a complete inventory of both private and public SSL certificates, and highlight any security issues.
3. Review and mitigate security issues – DigiCert will review any issues discovered with the customer and create a plan to mitigate issues found.
4. Handover workshop – Review the deployment and train customer personnel for on-going operation.
5. Customer sign-off on project completion.

CertCentral Automation deployment

The DigiCert CertCentral® Automation feature automates the process of installing, renewing, and replacing TLS/SSL certificates. From CSR generation to installation of the new certificates, certificate automation is becoming increasingly important for:

- **Large enterprises:** The industry is trending towards shorter and shorter certificate lifetimes which imply dramatically increasing labor costs—unless renewals can be automated. This will particularly impact larger enterprises with thousands of certificates.
- **Customers currently using other PKI platforms:** or other certificate vendors wishing to migrate/consolidate to DigiCert certificates.

We will work with your network and security teams to successfully deploy CertCentral Automation within your enterprise. Automation works with the most popular web servers and appliances. The process involves:

1. Planning workshop – Explain the solution and get buy-in from customer stakeholders.
2. Proof of Concept (POC) – DigiCert will demonstrate a working solution in the customer’s test environment.
3. Create automation strategy – DigiCert will develop a strategy to deploy automation and review/agree with the customer.
4. Deploy automation – DigiCert will work with the customer to configure automated renewal on all required/supported platforms.
5. Handover workshop – Review the deployment and train customer personnel for on-going operation.
6. Customer sign-off on project completion.

Training and certification workshops

We offer on-site or remote workshops covering DigiCert CertCentral TLS Manager and TLS/SSL Best Practices. In addition, students can choose to take the DigiCert Technical Certification exam to become certified in TLS/SSL or CertCentral. Three certification exams are currently available: one associate level and two professional levels. More information is available [here](#).

Associate
Level



Professional
Level

