

## DigiCert Products

A leading online trust provider, DigiCert offers multiple products to suit the security needs of enterprises within the finance, healthcare, education, government and Fortune 500® sectors. When compared to other Certification Authorities (CA) on the market, DigiCert provides the best value and flexibility with its Secured Socket Layer (SSL), code signing, S/MIME, Managed PKI, and other high-assurance certificates. For its efforts, the company has been recognized with dozens of awards for providing enhanced customer value, premium customer support and market growth leadership.

DigiCert's high validation standards enable our clients to earn the trust of their customers and grow their business without interruption. DigiCert played a key role in designing the CA/Browser Forum's Baseline Requirements and typically exceeds the minimum standards in issuing SSL certificates.

### SSL Certificates

DigiCert offers a variety of SSL certificate options designed to match the needs of organizations of all types, regardless of server type, number of servers, or number of domains an entity needs secured. Standard features with any DigiCert SSL certificate include:

- 2048-bit SSL Secure Sockets Layer with TLS Encryption
- Compatible with all major browsers
- Unlimited Free Reissues
- Unlimited Server License
- Solid vetting to ensure strong Authentication
- Secure Site Seal
- Phone, Email, and Chat Support
- Compatible with Apache, IIS, Tomcat, Exchange Server, and other servers
- Compatible with Linux, Windows and other operating systems

DigiCert leads the market by providing value-added items that set it apart from the competition and contribute to the company enjoying the strongest customer loyalty scores in the business.

### WILDCARD SSL CERTIFICATES

DigiCert's WildCard SSL certificates secure an entire domain using SANS technology. Every DigiCert WildCard SSL Certificate comes with an Unlimited Server License, so the customer only pays once, whether they have one server or one hundred.

Additionally, DigiCert offers its customers the option to obtain duplicate certificates issued to unique private keys/CSRs free of charge so that every server or certificate installation has a unique private key.

This is just one more way that DigiCert adds value by helping the user strengthen security across the entire network.

### STANDARD SSL CERTIFICATES

Single-name SSL certificates from DigiCert come with all the standard features that have created DigiCert's reputation for excellence. Additionally, these certificates include unlimited free reissues, professional site seals and a 30-day guarantee. With the DigiCert "Plus Feature" users are able to secure entire domains (i.e. www.example.com and example.com) with a single certificate.

### MULTI-DOMAIN (SAN) SSL CERTIFICATES

Multi-domain (SAN) certificates (sometimes known as SAN certificates), use Subject Alternative Names to let a company secure up to 25 fully-qualified domain names with one certificate. Every DigiCert multi-domain (SAN) certificate comes with an unlimited server license and “duplicate” feature, making them ideal for environments that need to secure multiple names across different domains. Plus, multi-domain (SAN) certificates are compatible with most platforms (e.g. Apache, Exchange, OCS, etc.).

### EXTENDED VALIDATION SSL CERTIFICATES

As SSL validation standards continue to improve, DigiCert is at the forefront of industry leadership offering Extended Validation SSL Certificates that create the ultimate level of trust for web users. Featuring the green navigation bar, companies can brand their trust with their customers and earn repeat business without interruption. DigiCert’s EV certificates use Subject Alternative Names to secure multiple domains (i.e. www.example.com and example.com in one SSL certificate).

## Code Signing

In August 2012, DigiCert introduced EV Code Signing for the first time in the internet security market. EV Code Signing Certificates from DigiCert are integrated with Microsoft’s SmartScreen® Application Reputation services to help software publishers gain immediate reputation in IE 9, IE 10 and Windows 8. Programs signed with an EV Code Signing Certificate can immediately establish reputation even if no prior reputation exists for their file or for them as a publisher. Reputation helps to reduce warning messages and instill confidence in users to run their application.

An EV digital signature from DigiCert helps protect software from malware, tampering, and theft, and combines the rigorous Extended Validation process with a hardware requirement to safeguard software companies’ business identity. DigiCert’s stringent verification can often be completed in hours instead of the days or weeks required by competitors. One of only two Certificate Authorities to offer EV Code Signing at its launch, DigiCert offers added-value with significant cost savings and award-winning customer support.

DigiCert offers EV and standard code signing certificates that work across a multitude of platforms including the most common ones such as Microsoft Authenticode & Kernel-mode signing, Java, Apple and Adobe. Code signing certificates from DigiCert allow customers to digitally sign software or applications, especially those that might be downloaded or run online, to verify that the code being run has not been altered or corrupted.

In general, a code signing certificate helps guarantee to users that they are, in fact, running the code they believe they are running, and that the code was written by the individual or organization to which the certificate was issued.

## Enterprise Managed PKI

Managed PKI (Public Key Infrastructure) allows organizations that require a large volume of SSL certificates to take control of ssl certificate management – including issuing new certificates and reissuing, replacing, and revoking existing SSL certificates – on-demand. The ability of an enterprise to manage its own PKI needs directly and immediately provides more control to the account administrator and eliminates the short waiting period associated with retail requests.

MPKI allows the organization to centralize control while diversifying workload. It also allows multiple sub accounts for different business units – e.g. the operations department could approve or reject requests from the programming department, or even limit them to certain domains (only allow programming to get certificates on test.example.com). The certificates are sent directly to the business units, so operations doesn't have to receive the certificate and install it – just control issuance.

DigiCert employs a strong support team of MPKI experts, including some of the most sought-after speakers within this growing industry.

### **Direct Project Compliant, Federally Bridged Certificates**

The 2014 implementation of the Affordable Care Act ushers in mandates associated with the department of Health & Human Services and its various sub-programs. A set of standards that governs the use of electronic health records (EHR), named Meaningful Use, allows eligible providers and hospitals to earn incentive payments for Medicare and Medicaid services by meeting specific criteria. Meaningful Use has a stated goal of promoting the expanded use of EHRs to improve healthcare in the U.S.

To help reach the goals of Meaningful Use, the Office for the National Coordinator for Health Information Technology (ONC) introduced the Direct Project in 2010 to encourage development of simple, secure and standards-based protocols and rules for securely exchanging electronic health records.

DigiCert is a founding member and current board member of DirectTrust, the leading non-profit

organization working to fulfill the Direct Project vision by providing a system for scalable trust. Under the banner of DirectTrust, DigiCert is the first Certification Authority to offer federally bridged, Direct-compliant certificates for healthcare exchange between federal and non-federal agencies. DigiCert certificates are also publicly trusted, follow global standards and protocols and are accredited at multiple levels of assurance within the DirectTrust Trust Bundle program. The Trust Bundle is designed to facilitate scalable trust by accrediting trust agents for the Direct program in compliance with a global set of standards. This helps eliminate the need for one-off contracts and fulfill the vision of scalable trust the Direct Project. As a pioneer in this market, DigiCert is working with government and private health organizations to implement Direct, federally bridged, secure messaging and offers an enterprise-level platform for health information service providers to utilize.

### **SecureWifi Certificates™**

DigiCert is one of only two trusted Certificate Authorities to provide digital certificates used in the WiFi Alliance's Release 2 of its Wi-Fi CERTIFIED™ Passpoint® program. DigiCert's SecureWifi Certificates authenticate and encrypt online signup servers compliant with Release 2 of its Wi-Fi CERTIFIED Passpoint program. DigiCert is a full-service provider and provides certificates to Wi-Fi chipset manufacturers, service providers, and access point vendors looking to participate in Passpoint. Additionally, authorized certificates from DigiCert can help retail and hospitality providers deploy Passpoint-certified networks at retail and hotel locations around the world.

Passpoint Release 2 features close some of the traditional gaps in hotspot security by provisioning online signup servers with an authorized digital certificate to authenticate the access point with the service provider's uniquely identifying common name and the provider's logo. This helps avoid user confusion and reduces the likelihood of a user falling prey to access point spoofing. Additionally, the use of an authorized certificate encrypts information exchanged during the signup process, helping to protect user's credentials when registering for a new account.

By streamlining the process for creating a new user account at the point of access, Passpoint helps to reduce barriers to account creation and usage for service providers. Likewise, it reduces the complexity for users in getting connected and enables them to re-connect easily across a service provider's broad network of hotspots with the trust that their credentials are securely exchanged when connecting.

The availability of SecureWifi Certificates, and subsequent work that DigiCert plans within the Wi-Fi Alliance in the coming future, represent an important step forward toward a vision of enabling secure Wi-Fi everywhere. With continued advancements in future Passpoint programs, the potential exists to enable globally available, authenticated hotspot access points and devices that are easily identifiable

and provisioned with end-to-end encryption. It also provides a path forward that may lead to expansion of global Wi-Fi roaming that reduces cellular data overload and demand for new cellular tower construction.

Mobile equipment vendors, operators and hospitality providers looking to participate in Release 2 features of the Passpoint program need to use an authorized digital certificate for certification. As the only publicly trusted Certificate Authority authorized for Release 2 of Passpoint, DigiCert invites participants to experience the DigiCert Difference™, which includes award-winning customer support, a host of products and tools to simplify and optimize digital certificate management, and fast negotiation of secure sessions designed for the speed of mobile business.

## SSL Installation, Checking, Discovery Tools

For many organizations with multiple servers and domains managing the certificate lifecycle can be a challenge. DigiCert offers a number of tools, including the DigiCert Certificate Inspector, DigiCert Certificate Utility, SSL Discovery Tool, SHA-1 Sunset Tool, Always-on SSL Checker, and other offerings that help simplify and automate key functions of the certificate lifecycle management process. Using DigiCert's tools, security engineers and administrators save valuable time and frustration to generate Certificate Signing Requests, install SSL and code signing certificates, check their SSL chain configuration, discover and renew certificates on their servers and various other tasks.

DigiCert leads the market in providing value-added tools that in many cases are available for little to no cost. Many of the company's tools are referenced by other CAs in communications with their customers.

## DigiCert Certificate Inspector

The DigiCert Certificate Inspector™ is designed to quickly find problems in certificate configuration and implementation, and provide real-time analysis of an organization's entire certificate landscape, including SSL termination endpoints. Using the tool, security professionals can discover forgotten, neglected or misconfigured certificates, and identify potential vulnerabilities, such as weak keys, problematic ciphers and expired certificates. For each potential threat detected, the tool provides a list of remediation activities.

SSL/TLS certificates are a key defense against unwanted surveillance of online user activity. Yet, too often system administrators fail to properly configure certificates, unknowingly leaving open vulnerabilities. Certificate Inspector scans the user's network detecting all certificates in use, inspects SSL configuration and implementation, and then displays the results in an intuitive and interactive dashboard.

By providing actionable information about certificate configuration and deployment status, combined with remediation tools, DigiCert helps organizations close the gap between certificate procurement and secure certificate deployment.

Security professionals can use the Certificate Inspector to:

- Establish their security baseline with a real-time, comprehensive overview of SSL certificates and their termination endpoints across the entire network.
- Detect vulnerabilities via scanning for problematic certificates or server configurations

and easily review results using Certificate Inspector's intuitive dashboard.

- Analyze security data points either by aggregate or specific to each certificate and endpoint.
- Mitigate discovered vulnerabilities, such as BEAST, and lack of compliance with industry guidelines such as the CA/Browser Forum Baseline Requirements, through recommended steps.
- Renew expiring certificates through DigiCert's express provisioning process.
- Archive snapshots from each detection event to document improvements over time.
- Run reports from any location with DigiCert's cloud-based administrative controls.

Using a proprietary algorithm, the Certificate Inspector analyzes SSL certificates and termination endpoints for many security factors, including:

- Weak keys, ciphers and hash algorithms
- SSL/TLS versions
- Expiring certificates
- TLS renegotiation
- Perfect Forward Secrecy
- Configuration vulnerability to CRIME, BREACH, BEAST, etc.
- Mismatched server/certificate names
- Missing AIA's

The Certificate Inspector is available to any security professional. To learn more about how to run reports and start optimizing their SSL configuration, administrators can visit <https://www.digicert.com/cert-inspector.htm>.

## Legally Binding Electronic Document Signing

DigiCert offers digital certificates to provision legally binding signatures of electronic documents. DigiCert Document Signing™ Certificates are approved by the Adobe® Approved Trust List for all Adobe products as well as for other popular document formats such as Microsoft® Word, LibreOffice® and OpenOffice®. The integrity of these signatures is protected for its users through multi-factor authentication. Within Adobe

documents, users can customize the appearance of their signatures to enhance the credibility and trust factor. DigiCert Document Signing Certificates are available at very competitive rates and are trusted everywhere.

**To learn more contact Jeff Chandler, PR Director at 1.801.701.9653, or 1.385.225.1207 or email [jeff.chandler@digicert.com](mailto:jeff.chandler@digicert.com).**