DIGICERT WEB PKI

CERTIFICATE TERMS OF USE

PUBLICLY TRUSTED TLS/SSL

1. Scope and Purpose

Short version: *These terms apply only to DigiCert's publicly trusted TLS/SSL certificates (DV, OV, EV, including wildcard TLS certificates). They incorporate DigiCert's Certificate Policy and Certification Practices Statement (CP/CPS), and reflect industry standards (like the CA/Browser Forum Guidelines and browser root store policies) that apply to publicly trusted TLS certificates.*

These terms ("Terms") apply to publicly trusted TLS/SSL certificates issued by DigiCert or its affiliates under DigiCert's Web PKI. They do not apply to other certificates outside DigiCert's Web PKI, including other certificate types or services (e.g., private/internal certificates, S/MIME e-mail certificates, code signing certificates, or EU qualified certificates). The Terms incorporate the DigiCert Public Trust CP/CPS (the "CP/CPS"), which together with these Terms set forth how Web PKI certificates are issued, managed, and revoked. The DigiCert Public Trust CP/CPS is available at https://www.digicert.com/legal-repository/, as updated from time to time (the "DigiCert Legal Repository"). These Terms reflect the policies and requirements established by industry authorities and the browsers, including the CA/Browser Forum's Baseline Requirements for publicly trusted TLS certificates, available at www.cabforum.org/working-groups/server/baseline-requirements/documents/ (the "Baseline Requirements"), and the Extended Validation (EV) Guidelines (for EV certificates), available at www.cabforum.org/working-groups/server/extended-validation/documents/ (the "EV Guidelines"). **As a Certification Authority ("CA"), DigiCert is obligated to abide by these industry standards, including promptly revoking certificates when required by applicable criteria in industry standards, without exception.**

2. Use of Web PKI Certificates

You may use your DigiCert TLS/SSL certificate only to secure the domain name(s) that you own or for which you have explicit authorization. The certificate may be installed on multiple servers or devices **only** if all those systems are under your control (for example, servers in your organization's infrastructure). **Keep the certificate's private key confidential.** Only you and your authorized agents should have access. Do not share your private key with outside parties.

These publicly trusted TLS certificates are intended **solely for TLS/SSL web server security.** You must not use a DigiCert TLS/SSL certificate for other purposes such as e-mail encryption, code signing, document signing, VPN authentication, or any use not sanctioned for public TLS certificates. Even if a certificate's technical properties might allow a certain usage, any such use that falls outside these Terms or the certificate's defined purpose is unauthorized and may violate industry compliance rules. Using a certificate for an out-of-scope or prohibited purpose is grounds for revocation (see **Revocation** section below).

3. Requesting a Certificate

Short version: *When you request a certificate, you promise that the info is true and that you're authorized to request the certificate for the domain and (if applicable) organization.*

When requesting a certificate, you must submit **accurate, complete, and truthful information**. This includes domain names, organization details, and any other data required for issuance. You

must **only request certificates for domain names that you own or control**, or for which you have the explicit permission of the owner. Do not include names, trademarks, or other information that you have no rights or authority to use.

By requesting a certificate, you represent and warrant that: **(a)** you have lawful rights or authority to use and control the domain names (and any organization name or personal names, if applicable) listed in the certificate request, and **(b)** your certificate request and intended use **will not infringe** upon the intellectual property or legal rights of any third party. Misuse of the enrollment process or providing any false, misleading, or unauthorized information is a material breach of these Terms. DigiCert will deny any certificate request that violates these rules, and **any certificate issued on the basis of false or misleading information may be revoked immediately.**

4. Verification Before Issuance

Short version: *DigiCert will verify your control of the domain(s) and, for OV and EV certificates, will also verify your organization. EV certificates require additional documentation and checks. If validation isn't successful or flags arise, DigiCert will not issue the certificate until the requirements are met.*

Before issuing any publicly trusted TLS certificate, DigiCert will perform the necessary identity and authorization checks, in accordance with its CP/CPS. All certificate requests are subject to final review and approval by DigiCert.

- **Domain Validation (DV, OV, EV):** For all certificate types, you must demonstrate control over the domain(s) to be included in the certificate. This may involve email-based challenges, DNS record creation, file uploads, or other approved domain control methods.
- **Organization Validation (OV, EV):** For OV and EV certificates, DigiCert must verify your organization's legal existence, operational status, and authority to request the certificate. This process may include review of official business registry records, address verification, phone call validation, and cross-checking with authoritative third-party sources.
- **Extended Validation (EV):** EV requests are subject to stricter criteria, including the designation of specific authorized roles (such as EV Requester, Approver, and Contract Signer) and additional documentation, such as legal registration evidence or professional opinion letters. DigiCert will verify these roles, confirm exclusive domain rights, and conduct enhanced fraud screening.

DigiCert may decline to issue a certificate if you fail to respond to validation inquiries, do not provide required documentation, or if DigiCert identifies a risk of fraud, misrepresentation, or non-compliance with industry standards. All validation steps must be completed to DigiCert's satisfaction before issuance. If a request cannot be validated or appears non-compliant, DigiCert will not issue the certificate.

5. How Long Certificates Last

Short version: *Certificates have short lifespans. You are responsible for replacing them before they expire. Using automation for certificate renewal is highly recommended.*

Public TLS/SSL certificates expire after a limited time by design. As of now, **the maximum validity** allowed for a publicly trusted TLS/SSL certificate is 398 days (about 13 months). Industry policies

are evolving to require even shorter lifespans in the coming years (e.g., a reduction to about 200 days in 2026, 100 days in 2027, and 47 days by 2029). These changes are driven by security best practices and CA/Browser Forum consensus to limit certificate lifetime, making automation essential. DigiCert may offer annual subscriptions or longer bundles for convenience, but certificates will still be re-issued at industry-mandated intervals (i.e., you will need to re-validate and install the updated certificate when required).

It is your responsibility to monitor the expiration date of each certificate and to obtain and install a replacement certificate before it expires. If a certificate expires, any systems relying on it will show errors or fail to connect securely. Expired certificates must not be used. Continuing to use an expired certificate is unsafe and violates these Terms. You should plan to remove or replace certificates promptly upon expiration.

DigiCert strongly recommends using certificate management automation (such as ACME protocols, DigiCert CertCentral® APIs, DigiCert Trust Lifecycle Manager, or other automated renewal tools) to handle renewals and replacements.

6. Your Responsibilities as a Subscriber

Short version: *By using or applying for a DigiCert certificate, you promise to uphold certain obligations. In summary, you must* ***(a)*** *provide accurate information,* ***(b)*** *protect your private key,* ***(c)*** *review and accept the certificate's contents,* ***(d)*** *use the certificate only as allowed (for the domains and purposes intended, and in compliance with law and policy),* ***(e)*** *promptly request revocation and cease use if the private key is compromised or if any certificate information becomes inaccurate,* ***(f)*** *stop using the certificate (and its key) upon expiration or revocation,* ***(g)*** *respond promptly to DigiCert's inquiries about security issues, and* ***(h)*** *acknowledge and agree to DigiCert's right to revoke the certificate when needed. These obligations are derived from industry standards that all subscribers must follow.*

As the Subscriber (certificate holder), you have important obligations to ensure the certificate is used securely and in accordance with these Terms, the CP/CPS, and applicable standards. **You hereby represent and warrant to DigiCert and to the Certificate Beneficiaries that you will do the following:**

a. **Accuracy of Information:** You will provide accurate and complete information at all times in your certificate request and in all communications with DigiCert related to your certificates. You will promptly update any information if it changes during the validation process. If any information you provided to DigiCert becomes outdated or incorrect (for instance, if your organization's name or address changes, or you cease to control a domain in the certificate), you will promptly update the information with DigiCert or notify DigiCert of the change.

b. **Protection of Private Key:** You will securely generate your certificate's private key using trustworthy systems and strong cryptographic standards (at least a 2048-bit RSA key or equivalent strength ECC, unless stronger requirements apply). You must keep the private key confidential and under your sole control at all times. This includes using all necessary measures to prevent the loss, disclosure, or unauthorized use of the private key.

c. **Acceptance of Certificate:** After DigiCert issues your certificate, you will review the certificate's details (such as the subject name, domain names, organization info, etc.) to ensure all information is correct. You will only use the certificate if you have verified that

the data in it is accurate and you accept it. Using the certificate signifies your acceptance of it. If you find any inaccuracies, you must contact DigiCert to revoke or reissue the certificate before using it.

d. **Use of Certificate:** You will install and use the certificate only on the server(s) or device(s) that are accessible by the domain name(s) listed in the certificate (i.e., the certificate's subjectAltName entries). You agree to use the certificate solely in compliance with these Terms, including the CP/CPS. The certificate must not be used on any system that you are not authorized to operate, and you must not use the certificate for any purpose other than its intended scope (see Use of Web PKI Certificates section above).

e. **Reporting and Revocation:** If you suspect or become aware of any actual or potential compromise of the certificate's private key, or any misuse of the certificate, you must immediately notify DigiCert and promptly request revocation of the certificate. Similarly, if any information in the certificate is or becomes false, inaccurate, or misleading at any time, then you must immediately cease using the certificate and promptly request DigiCert to revoke it.

f. **Termination of Use:** If a certificate is revoked for any reason, or if it reaches its expiration date, you must promptly remove the certificate from all your systems and cease all use of the certificate and its corresponding private keys. Using an expired or revoked certificate for any purpose is strictly prohibited. After a certificate has been revoked or expired, you also agree not to use the associated private key to circumvent the revocation.

g. **Responsiveness:** You will respond promptly to inquiries or instructions from DigiCert regarding your certificate or its related key. Timely cooperation may be critical to mitigate security threats or to comply with industry revocation requirements. Failure to respond to DigiCert's security inquiries or directions in a timely manner constitutes a breach of these Terms and could result in certificate revocation.

h. **Acknowledgment of Revocation Rights:** You acknowledge and accept that DigiCert, as a Certification Authority, has the right to revoke your certificate at any time, without prior notice if you violate these Terms, or if revocation is required to comply with DigiCert's CPS, applicable law, or industry standards. You agree that you will not object to or impede such revocation, and you waive any right to seek damages or remedies against DigiCert for a revocation that is conducted in accordance with these Terms. ***Industry standards sometimes require Certificate Authorities to revoke certificates on short notice; for example, within 24 hours for certain critical incidents, or within 5 days for other events. You acknowledge that DigiCert must adhere to these non-negotiable timelines, and you agree to act accordingly in such events.***

7. Revocation (When and Why)

Short version: *Some events require a certificate to be revoked before it normally expires. DigiCert must act fast to protect security and comply with industry standards. You are required to help and must not impede revocation.*

In some cases, you must request revocation (for example, if your private key is compromised or you no longer control a domain). In other cases, DigiCert must revoke a certificate even without your request, often on a short timeline. These revocation obligations are non-negotiable and

required by industry standards, including the Baseline Requirements and browser root store policies. The following timelines apply.

Revocation within 24 hours (required)

DigiCert will revoke certificates within 24 hours if any of the following occur:

a. You request in writing that DigiCert revoke the certificate.
b. You notify DigiCert that the original certificate request was unauthorized.
c. DigiCert obtains evidence that your private key has been compromised.
d. DigiCert is made aware of a demonstrated or proven method that can easily compute your private key based on the public key in the certificate.
e. DigiCert obtains evidence that the validation of domain authorization or control for any domain name or IP address in the certificate should not be relied upon.

Revocation within 5 days (required)

DigiCert will revoke certificates within 5 days if any of the following occur:

a. The certificate no longer complies with required technical standards (for example, its cryptographic or key size is no longer allowed under the Baseline Requirements or browser root store policy).
b. DigiCert obtains evidence that the certificate was misused.
c. DigiCert is made aware that you have breached a material obligation of these Terms.
d. DigiCert is made aware that use of any domain name or IP address in the certificate is no longer legally permitted (e.g., a court or arbitrator has revoked a domain name registrant's right to use the domain name).
e. DigiCert confirms that a wildcard certificate has been used to authenticate a fraudulent or misleading subordinate domain name.
f. DigiCert is made aware of a material change in the information originally contained in the certificate.
g. DigiCert is made aware that the certificate was not issued in full compliance with the Baseline Requirements or the CP/CPS.
h. DigiCert determines that the information appearing in the certificate is inaccurate.
i. DigiCert's right to issue certificates under the Baseline Requirements expires or is revoked or terminated, unless DigiCert has made arrangements to continue maintaining the CRL/OCSP repository.
j. Revocation is required by DigiCert's CP/CPS for a reason not covered above.
k. DigiCert is made aware of a demonstrated or proven method that exposes your private key to compromise or if there is clear evidence that the specific method used to generate the private key was flawed.

If DigiCert determines that revocation is required for any of the above reasons, it will proceed to revoke the certificate as soon as practicable. Certain high-severity threats require short-notice revocation. DigiCert adheres to the industry rule that it SHALL revoke within 24 hours for critical events, and SHALL revoke within 5 days for other enumerated events. In line with its CP/CPS and industry requirements, DigiCert will investigate problem reports promptly and **will not delay revocation** beyond the permitted timeline. If your certificate will be revoked or is revoked, DigiCert will usually send a notice to the contact email on record, with a brief explanation of the reason, as soon as reasonably possible. Once a certificate is revoked, it will be published as revoked in DigiCert's revocation repositories (CRL and/or OCSP), and it must be replaced with a

new certificate if service is to continue. You agree that DigiCert has the authority to revoke, and you accept the consequences of such revocation. DigiCert is not liable for any losses or damages you incur due to a revocation that is mandated by these Terms, the CP/CPS, or industry standards.

8. Certificate Transparency and Public Disclosure

Short version: *Whenever DigiCert issues a publicly trusted TLS/SSL certificate, certain details about the certificate (including your domain and possibly organization name) may be logged publicly in Certificate Transparency logs. This is an industry-promoted security measure. By using DigiCert certificates, you consent to this public disclosure of certificate information. Sensitive personal or account data is not included in these logs, but certificate data (like domain and company name) is public and permanent.*

DigiCert may log all issued TLS/SSL certificates to public Certificate Transparency (CT) logs in accordance with industry requirements and DigiCert's policies. CT logs are public databases of certificates used to monitor and audit certificate issuance across the industry. When your certificate is logged, the following information becomes visible to anyone (via CT search tools or data feeds): the certificate's serial number, the fully qualified domain name(s) (SANs) in the certificate, the issuance date, expiration date, the issuing CA, and for OV/EV certificates, your organization's name and location as included in the certificate. No confidential personal information (such as contact emails, payment info, or account IDs) is included in CT logs, only the information that is actually present in the certificate itself.

CT logging may happen as part of the issuance process (before or immediately after the certificate is delivered to you). **Once logged, a certificate's data cannot be retroactively removed from public logs.** Certificate Transparency data is effectively immutable and will remain accessible to the public indefinitely. The purpose of CT is to enhance security by allowing domain owners and the wider community to detect any mis-issued or fraudulent certificates quickly. By requesting a certificate from DigiCert, you acknowledge that certificate details will be published to CT logs and you consent to that publication. If you have concerns about certain information being public (for example, your organization's legal name), note that if it must appear in the certificate, it **will** become public via CT. You should **not request that optional information be included in a certificate if you are not comfortable with it being openly visible**. For instance, including an email address in a certificate's subjectAltName would mean that email address gets logged publicly. Generally, DigiCert certificates for TLS only include information that is necessary and not highly sensitive (domains and org names).

DigiCert may also maintain its own repositories and status services where certificate information and revocation status are available (e.g., OCSP responders, CRLs, and certificate status websites), as permitted by its CPS and the Baseline Requirements. These too are public-facing by design. By using the certificate, you acknowledge that its status (valid/revoked/expired) may be disclosed publicly through such mechanisms.

9. Unsupported Practices (Use at Your Own Risk)

Short version*: Some practices related to certificate usage are* ***strongly discouraged and not supported*** *by DigiCert. If you engage in these practices, you do so at your own risk, and DigiCert may not be able to support you or may not accommodate special requests arising from these choices. In particular, avoid hard-coding (pinning) certificates or keys in applications, and avoid trying to use one certificate for multiple incompatible purposes. Such practices can lead to service disruptions or non-compliance.*

Certain practices are **strongly discouraged or unsupported** when using DigiCert certificates. Engaging in these practices is at **your own risk**, and DigiCert's obligations to support or accommodate you may be limited if you do so:

- **Certificate/Key Pinning:** DigiCert does not support **hard-coding or "pinning"** of DigiCert certificates or public keys in applications, firmware, or devices. Pinning means your app or system is configured to trust only a specific certificate. Pinning a certificate can create rigidity. This can lead to outages or security risks (if you can't quickly replace the pinned certificate). If you choose to implement pinning with a DigiCert certificate, you assume full responsibility for any service disruptions that result. **DigiCert will not delay required actions** (including revocation) to accommodate a pinned environment.
- **Dual Use / Misuse of Certificates:** Do not rely on a single DigiCert certificate for multiple different usage scenarios that it was not designed for. For example, using one certificate for both TLS/SSL (web security) *and* another purpose like S/MIME email encryption, code signing, or client authentication is not supported. Each certificate is intended for a specific use case, as indicated by its type and extensions. Using certificates in unintended ways (even if technically possible) is **not recommended** and may result in security vulnerabilities or non-compliance with guidelines. If you use a certificate in an **unapproved manner**, you do so at your own risk. DigiCert is not responsible for any consequences of such use.
- **Irretrievable Embedding:** Avoid embedding certificates in a context where they cannot be readily replaced or revoked. For instance, burning a certificate into hardware firmware or widely distributed in a way that cannot be updated is risky. If that certificate expires or must be revoked, those devices may fail and there may be no way to fix it in the field.

You should only use DigiCert certificates in adherence to DigiCert's guidelines, the CP/CPS, and industry best practices. Any use of a certificate that makes it difficult for you or DigiCert to revoke or replace the certificate (such as deeply embedded certificates in hardware, or widespread pinning without backup plans) is done at your own risk. Always have a plan for rapid certificate replacement.

10. Miscellaneous

Integration with Other Agreements: These Terms, together with the CP/CPS, govern your use of TLS/SSL certificates provided by DigiCert. They are incorporated into, and supplement, the DigiCert Master Services Agreement (available at https://www.digicert.com/master-services-agreement) or other applicable service agreement between you and DigiCert. In the event of any conflict between these Terms and the CP/CPS, the provisions of the CP/CPS will prevail. In the event of any conflict between these Terms and any other agreements, service contracts, or terms applicable to DigiCert offerings, these Terms will prevail with respect to matters specifically relating to your use of DigiCert TLS/SSL certificates.

Relying Party Warranty and Third-Party Beneficiaries: Relying Parties and Application Software Vendors (as defined in the CP/CPS, and each, a "**Certificate Beneficiary**") are express third-party beneficiaries of your obligations and representations herein. DigiCert may offer a limited Relying Party Warranty for the benefit of persons who rely on a DigiCert certificate in good faith (for example, website visitors or users who suffer damage due to a certificate being improperly issued). Any such warranty is not a warranty to you as the Subscriber, but rather to third-party relying parties as defined in the CPS or warranty documentation. You are not a third-party

beneficiary of any such Relying Party Warranty. Aside from what is expressly stated in these Terms, there are no other third-party beneficiary rights conferred by this Terms of Use.

Modifications to Terms: DigiCert may update or modify these Terms from time to time to adapt to changes in services, technology, legal or regulatory requirements, or changes in industry standards. Updated versions of these Terms will be published on the DigiCert website (and/or through any in-product click-through, repository or communication channel) and will be indicated by an updated "Last Updated" date. DigiCert may also inform subscribers of significant changes through means such as email notifications or account alerts. By continuing to use Web PKI certificates or related services after these Terms have been updated, you signify your acceptance of the revised Terms. If you do not agree to the changes in the Terms, you should discontinue using the Web PKI certificates and related services (subject to any transitional provisions or grace periods that DigiCert may announce). It is your responsibility to review these Terms periodically for any updates. These Terms will remain in effect until all certificates issued under them have expired or been revoked and are no longer in use, or until the Terms are replaced by a newer version.

Plain Language Disclaimer: For convenience, some sections of these Terms include "Short version" summaries or simplified explanations to help illustrate the meaning of the section. These plain-language summaries are provided only to aid understanding and are not legally operative provisions. In case of any ambiguity or conflict between a summary and the full text of the Terms, the full, detailed text (and the incorporated CP/CPS) will govern. The use of plain language in these Terms is intended to make them easier to understand, but it does not diminish the legal enforceability of the provisions. The binding obligations of both you and DigiCert are as stated in the full text of the Terms.