digicert

DIGICERT X9 PKI

CERTIFICATE TERMS OF USE

1. Scope and Purpose

Short version: *These terms apply only to DigiCert's X9 PKI certificates. They incorporate the X9 CP, the DigiCert CPS, and reflect industry standards tailored for the high-assurance needs of the financial industry and similarly regulated environments. (They do* ***not*** *cover DigiCert's Web PKI certificates or any other non-X9 certificate services.)*

These Terms apply to X9 PKI certificates issued by DigiCert or its affiliates under the governance of the Accredited Standards Committee X9, Inc. (X9 ASC). They do not apply to certificates outside the X9 PKI, such as DigiCert's publicly trusted Web PKI certificates or other certificate types and services not governed by X9. These Terms incorporate the DigiCert X9 Financial PKI Certificate Policy and applicable policy documentation ("X9 CP") and DigiCert Certification Practices Statement for Private PKI (the "DigiCert CPS"), which together with these Terms set forth how X9 certificates are issued, managed, and revoked. The X9 CP is available upon request at https://x9.org/x9-financial-pki-qa/, as updated from time to time, with a copy for reference purposes only available at the DigiCert Legal Repository. The DigiCert 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 for the X9 PKI, which are intended to address the requirements of financial industry or other high-assurance PKI. (They differ from the CA/Browser Forum Baseline Requirements and other guidelines that apply to publicly trusted TLS certificates.)

2. Use of X9 Certificates

Short version: *You may use an X9 PKI certificate only for authorized use cases defined in the X9 CP and only within your authorized systems or domains. These use cases include, but are not necessarily limited to, those relevant to the financial sector.*

X9 certificates must only be used for the specific use cases authorized under the X9 CP and reflected in the certificate itself. Examples include:

- mTLS and client authentication
- Closed-network device authentication
- Secure API communication
- Digitally signed messages in the financial domain

X9 certificates are not intended for public TLS/SSL web PKI, public S/MIME e-mail, or other general purposes outside the X9 trust framework.

Certificates must only be installed on systems or services under your administrative control and used in accordance with the intended key usage and extended key usage extensions.

While the certificate's technical fields may support broader uses, only authorized PKI purposes are permitted. Use outside these constraints may result in revocation and is not supported. While X9 certificates are issued for defined purposes based on certificate type and profile as set forth in the X9 CP, DigiCert may, in consultation with the X9 Policy Authority, approve expanded or adjacent use cases that maintain consistent key usages (e.g., client authentication). Such

approvals must remain within the technical and security bounds of the X9 CP and may be subject to supplemental agreement, verification, or policy review.

3. Requesting a Certificate

Short version: *When you request an X9 certificate, you must provide truthful, accurate information and have authority to request a certificate for the entity, domain, and/or device identified.*

When requesting a DigiCert X9 PKI certificate, you must submit complete, accurate, and truthful information. You must be properly authorized to request a certificate for the organization, individual, device, and/or any domain name(s) or other identifiers included in your request. Do not submit certificate requests for domains or resources that you do not own or control, and do not include any information (such as organization names, trademarks, or other identifiers) that you are not authorized to use.

By submitting a certificate request, you represent and warrant that: (a) you have the lawful rights and authority to use and control all names, identifiers, and information (including any domain names, IP addresses, organization details, etc.) that you include in the certificate request; and (b) your request and the issuance of the certificate will not infringe upon or misappropriate the intellectual property rights or other legal rights of any third party. Any misuse of the enrollment process, any material misrepresentation of facts, or any provision of false or unauthorized information will result in denial of your request and may result in revocation of any certificate that might have been issued in reliance on such information.

4. Verification Before Issuance

Short version: *Either DigiCert or your institution (if acting as an RA) will perform identity checks before certificate issuance.*

X9 certificates may only be issued after successful identity and authorization verification, consistent with the X9 CP and applicable CPS. In some cases, your institution will act as a Registration Authority (RA), conducting verification internally in accordance with X9 standards. In other cases, DigiCert may perform these steps directly.

The specific procedures depend on the certificate type and intended use, and may include:

- Organization or domain validation
- Device or software identity checks
- Role-based authorization verification
- Cross-checks with government or industry data sources

All certificates are subject to DigiCert's final approval, even if your institution acts as the RA. DigiCert may decline to issue a certificate if it believes the request does not meet the X9 CP requirements or if it identifies a security or compliance concern.

5. Registration Authority Representations, Warranties, and Indemnity

If your organization acts as a RA, you represent and warrant that:

(a) You will perform all identity validation and certificate request functions in full compliance with the X9 CP, the applicable CPS, and these Terms;

(b) You have trained personnel, implemented appropriate background checks, and maintain secure infrastructure to fulfill your RA duties; and

(c) You will maintain accurate records and support audit rights as required under the X9 CP.

You agree to indemnify, defend, and hold harmless DigiCert Inc., its affiliates, and X9 ASC (and its Policy Authority) from any claims, damages, losses, liabilities, or costs (including reasonable attorneys' fees) arising out of or related to your acts or omissions as an RA, including without limitation: (i) failure to perform identity verification in accordance with the X9 CP, (ii) issuance or misrepresentation of certificate information, or (iii) unauthorized use or disclosure of private keys or applicant data.

6. How Long Certificates Last

Short version: *X9 certificates can be issued for longer periods than Web PKI certificates, but they still expire, and can never outlive the root certificate key that issued them. OCSP keys have a three-year maximum. Use automation to stay ahead of expirations.*

X9 certificates are issued for periods defined by your requirements, subject to the X9 CP and DigiCert CPS. However, all certificates expire and must be replaced before their expiration date to remain valid. In all cases, no certificate may have a validity period that exceeds the lifetime of the issuing CA's private key. Additionally, the maximum private key usage period for OCSP responders is limited under the X9 CP. DigiCert will enforce this and other lifecycle constraints as defined in the applicable certificate profiles and policies.

To avoid service interruption, you are responsible for tracking expiration and ensuring timely renewal or reissuance of all certificates in your environment. DigiCert strongly recommends implementing automated certificate lifecycle management using solutions like DigiCert® Trust Lifecycle Manager or other compatible tooling.

7. Your Responsibilities as a Subscriber

Short version: *You must safeguard your private key, use the certificate only as permitted (within its intended scope and systems), cease using it if any information becomes incorrect or it's compromised, and cooperate with DigiCert on any certificate-related inquiries. These obligations are required by X9 certificate policy and are crucial for security.*

As the Subscriber (as defined in the X9 CP), you have important obligations to ensure that the certificate is used securely and only in accordance with these Terms and the X9 CP. **By applying for or obtaining an X9 certificate, you agree, represent, and warrant to DigiCert that you have the authority to accept and bind your organization (if applicable) to these Terms (including the incorporated XP CP), and that you will do all of the following:**

(a) **Accuracy of Information:** Provide accurate and complete information at all times in your certificate request and in all communications with DigiCert related to the certificate's issuance and maintenance. If any information you provided becomes outdated or changes during the validation process or the certificate's validity period, you will promptly inform DigiCert or update the information as required.

(b) **Protection of Private Key:** Securely generate your certificate's private key using trustworthy systems and strong cryptographic standards (for example, at least a 2048-bit RSA key or an equivalent strength elliptic curve key, unless stronger requirements are defined by the X9 CP/CPS). You will take all reasonable measures to keep the private key

confidential and under your sole control. This includes using appropriate hardware or software security modules, protecting any passwords or tokens associated with the key, and preventing any unauthorized access to the private key. Do not share or disclose the private key to any unauthorized person.

(c) **Acceptance of Certificate:** Upon issuance of the certificate by DigiCert, promptly review the certificate's details (such as the subject name, organization information, domain names or other identifiers, and any other included data) to ensure everything is correct. If you discover any inaccuracies or issues, notify DigiCert immediately. You will only install or use the certificate after confirming that all details in it are accurate and that you accept the certificate.

(d) **Use of Certificate:** Install and use the certificate only on the server(s), device(s), software, or environment that is intended and authorized, as identified by the certificate's content. This means, for example, that a server TLS certificate should be installed only on the server(s) accessible by the domain name(s) or host identifiers listed in that certificate, an email certificate should be used only for the email address or user specified, and a code signing certificate should be used only to sign code on behalf of the organization or entity named. You agree to use the certificate only in compliance with all applicable laws and regulations, and solely in accordance with these Terms (including the incorporated X9 CP/CPS). The certificate may not be used on any system or by any entity other than those for which it was issued, and you must not use the certificate for any purpose other than securing the communications or transactions for which the certificate was intended.

(e) **Reporting and Revocation:** If you suspect that the certificate's private key has been compromised or exposed in any way, or if you become aware of any misuse of the certificate, you will promptly notify DigiCert and immediately request that the certificate be revoked. Similarly, if any information in the certificate is or becomes false, inaccurate, or misleading at any time (for example, if you no longer own or control a domain name included in the certificate, if your organization's name or address changes, or if any other detail in the certificate is no longer valid), you must immediately cease using the certificate and promptly request that DigiCert revoke the certificate. You should not wait for DigiCert or any other authority to detect such issues—initiation of revocation in these cases is your responsibility.

(f) **Termination of Use:** If a certificate is revoked for any reason, or when a certificate reaches its expiration date, you must promptly remove the certificate from all devices and systems on which it was installed and cease all use of the certificate and its associated private key. Using an expired or a revoked certificate (for any purpose) is strictly prohibited. Additionally, after a certificate has been revoked or has expired, you agree not to use the corresponding private key to issue new signatures or in any way that relies on the trust of the revoked/expired certificate. Once a certificate is no longer valid (either due to revocation or expiration), both the certificate and its key should be considered retired from service.

(g) **Responsiveness:** You will respond promptly to any inquiries or instructions from DigiCert regarding the certificate or its use. For example, if DigiCert contacts you to investigate a potential compromise, misuse, or any complaint regarding your certificate, you agree to reply and cooperate within the timeframe specified by DigiCert. Timely

cooperation may be necessary to address security incidents or compliance issues and is a condition of your continued certificate use.

(h) **Acknowledgment of Revocation Rights:** You acknowledge and agree that DigiCert, as an X9-authorized Certification Authority, has the right to revoke your certificate in accordance with the X9 CP. In particular, your certificate may be revoked in the event of a private key compromise, material changes in the information contained in the certificate, or any other circumstance that renders the certificate unreliable or non-compliance with the X9 CP. DigiCert is authorized to perform such a revocation with immediate effect and without prior notice when necessary to protect the security of the PKI or to comply with applicable requirements. In the event of a revocation, DigiCert will provide you with a notice of the revocation and a brief explanation of the reason as soon as practicable thereafter, consistent with the X9 CP's procedures.

8. Revocation (When and Why)

Short version: *X9 certificates can be revoked by DigiCert upon Subscriber request or if a certificate poses a security risk. The revocation process follows the X9 CP and may differ from DigiCert's public Web PKI practices (e.g., timing and criteria for revocation).*

Under the X9 CP, DigiCert may revoke an X9 certificate for a variety of reasons, including:

(a) **Private Key Compromise or Suspected Compromise:** If the certificate's private key is known or believed to be compromised, DigiCert will revoke the certificate to protect the integrity of the PKI.

(b) **Material Changes or Inaccurate Information:** If any information in the certificate becomes materially false or misleading. For example, if the Subscriber's organization name or control has changed such that the certified details are no longer detailed, the certificate will be revoked.

(c) **Misuse or Policy Violation:** If a certificate is misused (used outside of the permitted X9 use cases or contrary to these Terms and the X9 CP) or if the Subscriber breaches their obligations, DigiCert may revoke the certificate. Any circumstance that renders the certificate non-compliant with the X9 CP or otherwise unreliable will result in revocation.

(d) **Upon Subscriber's or Authorized Request:** DigiCert will revoke an X9 certificate upon request by the Subscriber (or an authorized organizational representative or RA) after verifying the authenticity of the request.

(e) **Security or Compliance Requirement:** DigiCert may revoke a certificate if required to comply with law, regulation, or at the direction of the X9 Policy Authority, or if continuing to trust the certificate could adversely affect the security of the X9 PKI environment.

In addition to revocation, DigiCert reserves the right to suspend certificates (i.e., temporary certificates), subject to and according to the requirements of the X9 CP, while investigating an issue. The suspended certificate may later be fully revoked or reinstated as appropriate.

9. Miscellaneous.

Integration with Other Agreements: These Terms, together with the DigiCert X9 PKI CP and the DigiCert CPS, govern your use of X9 certificate services 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 X9 CP, the provisions of the CP will prevail. In the event of any conflict between these Terms and any other agreements, service contracts, or terms applicable to DigiCert offerings that you may have, these Terms will prevail with respect to matters specifically relating to your use of X9 certificates.

No Third-Party Beneficiaries: There are no third-party beneficiaries to these Terms.

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 the X9 PKI policies or 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 X9 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 X9 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 X9 CP) 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.