DIGICERT E-MAIL PKI

CERTIFICATE TERMS OF USE

PUBLICLY TRUSTED S/MIME CERTIFICATES

1. Scope and Purpose

Short version: *These terms apply only to DigiCert's publicly trusted S/MIME certificates. They incorporate DigiCert's Certificate Policy and Certification Practice Statement (CP/CPS) and reflect industry standards (like the CA/Browser Forum S/MIME Baseline Requirements and root store policies such as Mozilla's) that apply to publicly trusted S/MIME certificates.*

These terms ("Terms") apply to publicly trusted S/MIME certificates issued by DigiCert or its affiliates. They do not apply to TLS/SSL (browser-trusted) certificates, private/internal S/MIME, code signing, document signing, or EU qualified certificates. The Terms incorporate the DigiCert Public Trust CP/CPS (the "CP/CPS"), available at https://www.digicert.com/legal-repository/, which together with Terms sets forth how S/MIME certificates are issued, managed, and revoked. These Terms reflect the policies and requirements established by the CA/Browser Forum S/MIME Baseline Requirements available at www.cabforum.org/working-groups/smime/documents/ ("Baseline Requirements") and applicable root store policies (e.g., Mozilla, Microsoft, Apple). **As a Certification Authority ("CA"), DigiCert is obligated to abide by these industry standards, including promptly revoking certificates when required, without exception.**

2. Use of S/MIME Certificates

You may only use DigiCert S/MIME certificates to secure email in connection to signing, encryption, and related client authentication. You may not use them for TLS/SSL web servers, code signing, document signing, or other unrelated purposes.

Permitted uses:

- Signing email to authenticate the sender and message integrity
- Encrypting email to provide confidentiality
- Client authentication, if consistent with the certificate's extensions and policies

Prohibited uses:

- TLS/SSL (web server authentication)
- Code signing or document signing (unless specifically designated)
- Any use outside the intended scope

Using a DigiCert S/MIME certificate for a prohibited purpose is grounds for revocation (see **Revocation** section below).

3. Requesting a Certificate

Short version: *When you request an S/MIME certificate, you promise that the info is true and that you're authorized to request it for the email address/domain and (if applicable) organization.*

When requesting a certificate, you must submit accurate, complete, and truthful information. This includes the email address, organization details, and any other data required for issuance.

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 control of the email address (or domain), and for certain certificate types will also verify the individual or organization.*

Before issuing any publicly trusted S/MIME certificate, DigiCert will perform the required validation steps in accordance with the CP/CPS and the Baseline Requirements. These include:

- **Mailbox-validated (MV):** DigiCert verifies control of the email address to be included in the certificate. This may involve sending a verification email challenge, requiring a DNS record for the domain, or other approved mailbox control methods. DigiCert also checks DNS CAA records for any "issuemail" property that permits or forbids issuance.
- **Organization-validated (OV):** In addition to email control, DigiCert verifies the organization's legal existence, operational status, and authority to use the email domain. This may include checking official registry records, performing address and phone verification, and cross-checking third-party sources.
- **Sponsor-validated (SV):** DigiCert validates the email address and confirms that the organization has sponsored the individual certificate holder. The sponsor organization must be verified and must designate the applicant.
- **Individual-validated (IV):** DigiCert verifies the natural person's identity, typically through a government-issued photo ID, notarization, or equivalent method, and verifies control of the email address.

If DigiCert cannot complete validation to its satisfaction, it will not issue the certificate. DigiCert may also decline issuance if there is a risk of fraud or non-compliance with industry standards or its processes.

5. Registration Authority ("RA") Representations, Warranties, and Indemnity

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

a. You will perform all identity validation and certificate request functions in full compliance with the CP/CPS, Baseline Requirements 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 CP/CPS and Baseline Requirements.

You agree to indemnify, defend, and hold harmless DigiCert and its affiliates and their respective directors, officers, agents, employees, successors and assigns 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 CP/CPS, Baseline Requirements and these Terms, (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: *Certificates have limited lifespans. The maximum allowed is 825 days (about 27 months). You must replace them before they expire.*

Publicly trusted S/MIME certificates expire after a limited time. As of now, the maximum validity permitted under the Baseline Requirements is 825 days. Industry practices may evolve to require short lifecycles in the future. DigiCert may offer subscription terms for convenience, but certificates will still be reissued at industry-mandated intervals.

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 automation (such as CertCentral® APIs, Trust Lifecycle Manager, or other automated tools) to handle renewals and replacements.

7. Your Responsibilities as a Subscriber

Short version: *By using or applying for a DigiCert S/MIME 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 validated email address 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 (except that you may retain the key solely to decrypt previously received mail where permitted),* ***(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 your S/MIME 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 S/MIME certificates. You will promptly update any information if it changes during validation. If any information you provided becomes outdated or incorrect (for instance, if your legal name, organization name or address changes, or you cease to control or lawfully use an email address included 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 permitted by the Baseline Requirements**). You must keep the private key confidential and under your sole control at all times, using measures sufficient to prevent loss, disclosure, or unauthorized use (e.g., strong passphrases, secure keystores or tokens, appropriate device and account controls). You are responsible for retaining access to private keys used for **email decryption** so you can read previously received encrypted messages; where permitted by policy and law, maintaining a secure backup/escrow for decryption keys is recommended. (Do not share your private key with third parties except as allowed by the CPS, such as through an approved enterprise key management mechanism.)

c. Acceptance of Certificate. After DigiCert issues your certificate, you will review the certificate's details (such as the subject name, rfc822Name email address(es), and any organization info) 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 your own email clients, devices, and systems (or those you are authorized to operate) that send and/or receive mail for the validated email address(es) listed in the certificate. You agree to use the certificate solely in compliance with these Terms (including the CP/CPS). The certificate must **not** be used for any purpose other than its intended scope (i.e., **email signing and encryption** and related client authentication) and must **not** be used for server TLS/SSL, code signing, document signing (unless explicitly profiled), or any other out-of-scope use.

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 (including phishing, fraud, or other unlawful use), 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 (for example, an email address is reassigned/retired or organization details change), 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 systems and **cease all use** of the certificate and of that private key for signing or presenting trust to relying parties. Using an **expired or revoked** certificate for any purpose that asserts ongoing trust is strictly prohibited. *For the avoidance of doubt:* retaining the private key **solely to decrypt previously received email** (or for lawful archival/records obligations) is permitted where allowed by policy and law; you must not use the key to continue signing email or to otherwise circumvent revocation or expiry.

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 may 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 CP/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 conducted in accordance with these Terms. ***Industry standards require CAs to revoke certificates on short notice (for example, within 24 hours for certain critical incidents and within 5 days for other enumerated events). You acknowledge that DigiCert must adhere to these non-negotiable timelines and agree to act accordingly in such events.***

8. 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 an e-mail address). 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 applicable root store policies (e.g., Mozilla Policy). 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 subject identity information 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 applicable 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 obtains evidence that the validation of control for any email address or domain part in the certificate should not be relied upon.
e. DigiCert is made aware of a material change in the information originally contained in the certificate.
f. DigiCert is made aware that the certificate was not issued in full compliance with the Baseline Requirements or the CP/CPS.
g. DigiCert determines that the information appearing in the certificate is inaccurate.
h. 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.
i. Revocation is required by DigiCert's CP/CPS for a reason not covered above.

j. 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.

9. Public Disclosure

DigiCert may 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 are public-facing by design. By using the certificate, you acknowledge that its status (valid/revoked/expired) may be disclosed publicly through such mechanisms.

10. 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 S/MIME email encryption *and another purpose like* TLS/SSL (web security) *and* 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.

11. Miscellaneous

Integration with Other Agreements: These Terms, together with the CP/CPS, govern your use of S/MIME 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 S/MIME 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, email recipients 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 the 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 S/MIME 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 S/MIME 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.