SERVICE SPECIFIC TERMS / CLOUD

SSL Certificates

SSL/TLS certificates from public Certificate Authorities

VERSION	EFFECTIVE	REPLACES
v2026.11a	1 November 2026	SSL.pdf

These Service Specific Terms form part of your agreement with FirstNet Technology Services (Pty) Ltd. Read them with the FirstNet Standard Terms and Conditions (or your signed Master Services Agreement), your Service Schedule and the Data Processing Annexure, all available at www.firstnet.co.za/legal-notices/.

Publicly trusted SSL/TLS certificates (DV, OV, EV, wildcard and multi-domain), supplied unmanaged or managed

1. Status and precedence

1.1 These Service Specific Terms ("SST") apply to every SSL/TLS certificate that FirstNet Technology Services (Pty) Ltd (registration number 2006/031608/07) ("FirstNet") obtains for the Customer, and to any related installation or management service.

1.2 These SST form part of the agreement between FirstNet and the Customer, which is either the FirstNet Standard Terms and Conditions or the Customer's signed Master Services Agreement with FirstNet (the "Agreement"). They are incorporated into the Agreement by reference and are published at www.firstnet.co.za/legal-notices/.

1.3 What the Customer has ordered (the Certificate Authority or brand, Validation Type, the domain names to be covered, the Subscription Term, whether the service is Managed or Unmanaged, and the Charges) is set out in the Service Schedule, quote or scope of work signed or accepted by the Customer (the "Service Schedule").

1.4 If documents conflict, they apply in this order: (a) the Service Schedule, but only for commercial items it expressly overrides; (b) these SST; (c) the Agreement (including the Data Processing Annexure and the Acceptable Use Policy); (d) the Vendor Terms. Where the Vendor Terms or the Industry Requirements impose a mandatory rule on the issue, use or revocation of a Certificate, that rule applies and the Customer must comply with it.

1.5 Words defined in the Agreement have the same meaning in these SST.

2. Definitions

2.1 **"Certificate"** means a publicly trusted digital certificate in the X.509 format, issued and digitally signed by a Certificate Authority, that binds a Public Key to one or more domain names (and, for OV and EV Certificates, to the verified identity of an organisation), so that browsers and other software can authenticate the server and set up an encrypted TLS (Transport Layer Security, often still called "SSL") connection. A Certificate is not itself an encryption algorithm and does not by itself encrypt or secure anything.

2.2 **"Certificate Authority"** or "CA" means the organisation that issues the Certificate, as named in the Service Schedule (see clause 3.2).

2.3 **"CSR"** means a certificate signing request: a file generated with the Key Pair that contains the Public Key and the details to be included in the Certificate.

2.4 **"DCV"** means domain control validation: the CA's check that the applicant controls each domain name to be included in the Certificate, usually by a DNS TXT or CNAME record, an email to a prescribed address, or a file placed on the website.

2.5 **"Industry Requirements"** means the rules that a CA must follow to issue publicly trusted Certificates, including the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, the CA/Browser Forum Extended Validation Guidelines, and the root programme rules of browser and operating system vendors, as amended from time to time.

2.6 **"Key Pair"** means a Private Key and its matching Public Key.

2.7 **"Managed"** means that, as recorded in the Service Schedule, FirstNet generates the CSR, completes DCV and installs the Certificate on servers that FirstNet manages for the Customer.

2.8 **"Private Key"** means the secret half of a Key Pair, which must be kept confidential; whoever holds it can impersonate the Customer's server.

2.9 **"Public Key"** means the half of a Key Pair that is included in the Certificate and may be published.

2.10 **"Subscriber Agreement"** means the CA's subscriber agreement or certificate terms of use listed in clause 4, which the Customer accepts as the subscriber of the Certificate.

2.11 **"Subscription Term"** means the period paid for by the Customer and stated in the Service Schedule (for example one year), during which FirstNet will obtain Certificates for the covered domain names as set out in clause 3.5. The Subscription Term is not the same as the Validity Period of an individual Certificate.

2.12 **"Unmanaged"** means that, as recorded in the Service Schedule, the Customer (or its hosting provider) generates the CSR, completes DCV (unless FirstNet hosts the DNS) and installs the Certificate. Unless the Service Schedule expressly says the service is Managed, it is Unmanaged.

2.13 **"Validation Type"** means:

2.13.1 DV (domain validated): the CA verifies control of the domain names only;

2.13.2 OV (organisation validated): the CA also verifies the legal existence, name and address of the Customer's organisation; and

2.13.3 EV (extended validation): the CA verifies the Customer's organisation to the stricter standard of the CA/Browser Forum Extended Validation Guidelines.

2.14 **"Validity Period"** means the period between the "not before" and "not after" dates written into a Certificate.

2.15 Certificates may cover one fully qualified domain name, a wildcard (for example *.example.co.za, which covers one level of sub-domains) or several named domain names (a multi-domain, SAN or UCC Certificate), as stated in the Service Schedule.

3. Service description

3.1 What FirstNet provides. FirstNet acts as a reseller of Certificates. FirstNet will:

3.1.1 order the Certificate of the brand, Validation Type and coverage stated in the Service Schedule from the CA, on the Customer's behalf and in the Customer's name;

3.1.2 submit the Customer's CSR and organisation details to the CA and guide the Customer through DCV and, for OV and EV, organisation validation;

3.1.3 where FirstNet hosts the Customer's DNS, add the DNS records needed for DCV;

3.1.4 deliver the issued Certificate and its intermediate certificates only to the approved recipient named by the Customer; and

3.1.5 for a Managed service only, generate the Key Pair and CSR, complete DCV and install the Certificate on the servers named in the Service Schedule that FirstNet manages for the Customer. FirstNet does not keep a copy of the Private Key after the Certificate is installed.

3.2 Who issues the Certificate. The Certificate is issued by the CA, not by FirstNet. FirstNet currently sources Certificates from:

3.2.1 GoDaddy, whose Certificates are issued by GoDaddy's certificate authorities operated by Starfield Technologies, LLC; and

3.2.2 The SSL Store, a certificate reseller that supplies Certificates of several CA brands (for example Sectigo and DigiCert).

The CA for each Certificate is named in the Service Schedule or in the order confirmation. FirstNet may change the CA or brand used for a future Certificate or reissue (for example if a CA is distrusted by browsers) on notice to the Customer, provided the replacement is of the same or a higher Validation Type and coverage.

3.3 Validation. Issue of every Certificate depends on the CA completing its validation under the Industry Requirements. For OV and EV Certificates the Customer must provide the company documents and contact verification that the CA asks for. The CA decides whether to issue. FirstNet does not guarantee that a Certificate will be issued, or how long validation will take.

3.4 Validity Periods. Each Certificate is issued with the Validity Period that the CA sets, which may not exceed the maximum allowed by the Industry Requirements at the time of issue. The CA/Browser Forum has adopted a schedule that progressively reduces the maximum Validity Period of publicly trusted TLS Certificates and the period for which a CA may reuse a previous DCV, and these limits may be reduced further. As a result, a Certificate will often expire before the end of the Subscription Term, and DCV may have to be repeated more often.

3.5 Reissue within the Subscription Term. Where a Certificate expires, or must be replaced because of a change in the Industry Requirements or a revocation that is not caused by the Customer, before the end of the Subscription Term, FirstNet will obtain a replacement Certificate for the same domain names and Validation Type for the rest of the Subscription Term at no additional Charge, unless the Service Schedule states a reissue Charge. The Customer must complete any new DCV and, for an Unmanaged service, install each replacement Certificate before the previous one expires. FirstNet will remind the Customer's technical contact before a Certificate is due to expire.

3.6 Unmanaged service (default). For an Unmanaged service, the Customer is responsible for generating the Key Pair and CSR, completing DCV (unless FirstNet hosts the DNS), installing the Certificate and its intermediate certificates, configuring its servers, and testing the installation. The Customer should install and test each Certificate within 7 (seven) Business Days of delivery and tell FirstNet promptly of any problem with the Certificate itself. FirstNet will not install a Certificate on a server that it has not been contracted to manage.

3.7 Managed service. For a Managed service, FirstNet will install the Certificate on the servers named in the Service Schedule in a change window agreed with the Customer, and test that the Certificate is served correctly. The Customer must give FirstNet the access and cooperation needed. Installation involves changes to the Customer's server configuration; FirstNet will use reasonable care and, where practical, keep the previous configuration so that it can be rolled back.

3.8 What is not included. Unless the Service Schedule says otherwise, the Service does not include: installation on servers FirstNet does not manage; troubleshooting the Customer's servers, applications, load balancers or hosting provider; website security testing; code signing, S/MIME (email), client or document signing certificates; or advanced electronic signatures under ECTA (see clause 13.3).

4. Vendor Terms

4.1 The Customer is the subscriber of each Certificate. The CA's Subscriber Agreement governs the Certificate and the relationship between the CA and the Customer. The Customer accepts the Subscriber Agreement of the CA that issues its Certificate when it orders the Certificate, and authorises FirstNet to accept it on the Customer's behalf where the CA's ordering process requires FirstNet to do so. The current Subscriber Agreements are:

4.1.1 GoDaddy: Certificate Services Agreement (https://www.godaddy.com/legal/agreements/certificate-services-agreement), SSL Certificate Service Subscriber Agreement of Starfield Technologies, LLC (https://certs.godaddy.com/repository/certificate_practices/en/StarfieldSubscriberAgreement.pdf), and the certificate policy and practices documents in the GoDaddy repository (https://certs.godaddy.com/repository);

4.1.2 Sectigo: Sectigo Certificate Subscriber Agreement (https://www.sectigo.com/uploads/legal/Certificate-Subscriber-Agreement-3.1-click.pdf) and the Sectigo legal repository (https://www.sectigo.com/legal);

4.1.3 DigiCert: Digital Certificates by DigiCert, Terms of Use (https://www.digicert.com/content/dam/digicert/pdfs/legal/Certificate-Terms-of-Use.pdf) and the DigiCert legal repository (https://www.digicert.com/legal-repository); and

4.1.4 for any other CA brand supplied through The SSL Store, that CA's subscriber agreement as presented in the ordering process or as provided or linked by FirstNet.

4.2 The Subscriber Agreements impose obligations on the Customer, including those summarised in clause 5.3. A summary in these SST does not replace the Subscriber Agreement, and the Customer must comply with the Subscriber Agreement as amended by the CA from time to time.

4.3 A CA may change its products, Subscriber Agreement, validation methods or practices, and may be required to do so by changes to the Industry Requirements. FirstNet is not liable for those changes. Where a change materially affects the Service, FirstNet will tell the Customer.

4.4 A CA may refuse to issue, or may revoke, a Certificate under its Subscriber Agreement, its certification practice statement or the Industry Requirements. FirstNet is not liable for that refusal or revocation.

4.5 FirstNet passes through to the Customer the CA's warranties (and any relying party warranty the CA offers) only to the extent FirstNet may do so. Any claim under those warranties is against the CA. FirstNet gives no additional warranty for the Certificate.

4.6 Licence. The right to use a Certificate is granted by the CA to the Customer under the Subscriber Agreement, and is non-exclusive and non-transferable. FirstNet does not grant a separate licence. All intellectual property in the Certificate, the CA's keys and the CA's trademarks and site seals remains with the CA or its licensors.

5. Customer responsibilities

5.1 Authority. By ordering a Certificate, the Customer authorises FirstNet to: (a) apply for and buy the Certificate on its behalf and in its name; (b) give the CA the information about the Customer, its organisation and its contacts that the CA needs to validate and issue the Certificate; (c) for a Managed service, generate the Key Pair for the Customer's server; and (d) request revocation of the Certificate where clause 11 allows.

5.2 Customer warranties. The Customer warrants that: (a) all information it gives FirstNet or the CA is accurate, complete and current, and the CA and FirstNet may rely on it; (b) it owns or controls, or has the authority of the owner of, each domain name and organisation name to be included in the Certificate; and (c) its use of the Certificate will not infringe the rights of any third party.

5.3 Subscriber obligations. The Customer must, and must ensure that its staff, contractors and hosting providers:

- 5.3.1 use each Certificate only on servers accessible at the domain names listed in it, and only on behalf of the organisation named in it, for lawful purposes and in accordance with the Subscriber Agreement;
- 5.3.2 keep the Private Key confidential and protected, and not share it except with the persons who need it to install and operate the Certificate;
- 5.3.3 not modify a Certificate, and not use the Private Key to sign other certificates;
- 5.3.4 tell FirstNet immediately, and request revocation, if the Private Key is or may be compromised, if any information in the Certificate becomes inaccurate or misleading (including a change of organisation name or loss of control of a domain name), or if the Certificate is being misused;
- 5.3.5 stop using a Certificate and its Private Key, and remove it from all servers, when it expires or is revoked;
- 5.3.6 respond promptly to any instruction from FirstNet or the CA relating to validation, reissue or revocation. The Industry Requirements require CAs to revoke Certificates within short periods in some circumstances (in some cases within 24 hours or 5 days), so the Customer must be able to replace a Certificate at short notice; and
- 5.3.7 where it publishes CAA DNS records, keep them consistent with the CA used for its Certificates (FirstNet will update them where it hosts the DNS).

5.4 Private Keys generated by FirstNet. For a Managed service, FirstNet will take reasonable steps to keep the Private Key confidential, will transfer it only over a secure channel, and will not keep copies beyond what its managed configuration backups require.

5.5 Domain names. A registered domain name is needed for each Certificate. The Customer remains responsible for renewing its domain names; a Certificate cannot be issued or reissued for a domain name that has expired.

6. Provisioning and lead times

6.1 FirstNet will place the order after the Service Schedule is approved and any required payment is received. DV Certificates are usually issued shortly after DCV is completed. OV and EV Certificates usually take longer because of organisation validation. Lead times are indicative only and depend on the CA and on how quickly the Customer completes validation steps.

6.2 FirstNet delivers Certificate files only to the approved recipient named in the Service Schedule or in the Customer's written instruction, by encrypted email or another secure method. FirstNet is not responsible for delay caused by an incorrect or unavailable recipient.

7. Service levels and support

7.1 The Certificate is a product of the CA. Its availability, the CA's revocation-checking services (OCSP and CRL) and the trust placed in it by browsers and operating systems are outside FirstNet's control. No FirstNet availability target applies to them.

7.2 For a Managed service, any service levels for the managed servers are as stated in the Service Schedule for those servers.

7.3 Support requests are logged by email to support@firstnet.co.za or by telephone on 0861 989 896.

7.4 Service credits apply only if the Service Schedule states them. Where they apply, they are the Customer's sole financial remedy for the failure concerned. This does not limit the Customer's right to terminate the affected Service for material or repeated breach under the Agreement.

8. Data, privacy and security

8.1 Personal information shared with the CA. To issue a Certificate, FirstNet gives the CA the names, email addresses and telephone numbers of the Customer's contacts and, for OV and EV, company details. The CA processes this information as a responsible party under its own privacy policy. The CAs FirstNet uses are based outside South Africa (for example in the United States or the United Kingdom) and may process this information outside South Africa. FirstNet makes this transfer only where section 72(1) of the Protection of Personal Information Act 4 of 2013 ("POPIA") allows it, in particular where the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject (section 72(1)(d)), or where the CA is subject to a law, binding corporate rules or a binding agreement that provides an adequate level of protection (section 72(1)(a)). The Customer must make sure that its contacts are informed that their information will be shared with the CA for this purpose.

8.2 Public information. The information in a Certificate (including domain names and, for OV and EV, the organisation name and location) is public. CAs must log publicly trusted TLS Certificates in public Certificate Transparency logs, where anyone can see the domain names they cover. The Customer must not include domain or host names in a Certificate that it wants to keep confidential.

8.3 FirstNet as operator. Where FirstNet manages servers for the Customer under a Managed service, FirstNet processes any personal information on those servers as the Customer's operator, under the Data Processing Annexure published at www.firstnet.co.za/legal-notices/ and the Service Specific Terms for those servers.

8.4 No guarantee of security. A Certificate enables an encrypted connection between a browser and the server on which it is installed. It does not make the website, server or application secure, and does not protect data before it reaches, or after it leaves, that encrypted connection. In particular, FirstNet does not warrant that: (a) the Certificate will operate without error or interruption; (b) the Customer's website or transactions are secure or reliable; or (c) information transmitted through the Customer's website is protected from theft, interception or alteration.

9. Fees, licences and changes

9.1 The Charges for each Certificate and for any Managed installation are set out in the Service Schedule. These SST do not state prices.

9.2 Certificate Charges are paid for the whole Subscription Term in advance, unless the Service Schedule says otherwise. Because the Certificate is bought from the CA when ordered, Charges are not refundable once the CA has issued the Certificate, except to the extent the CA's own refund policy allows a refund to FirstNet, which FirstNet will pass on.

9.3 Certificate prices are often set by the CAs in US dollars. FirstNet may change the Charges for a new order or for the next Subscription Term to reflect CA price changes or exchange rates. FirstNet will tell the Customer of the renewal price in its renewal notice.

9.4 Installation on servers that FirstNet does not manage, troubleshooting of the Customer's servers, and additional reissues that are not covered by clause 3.5 (for example because the Customer lost its Private Key or needs a Certificate for different domain names) are chargeable at FirstNet's then-current rates after the Customer approves a quote.

10. Term, cancellation and early termination

10.1 The Service for each Certificate starts when FirstNet places the order with the CA and runs for the Subscription Term.

10.2 Renewal. FirstNet will send a renewal notice with the renewal price to the Customer's billing and technical contacts before the end of the Subscription Term, early enough for the Customer to approve the renewal and complete any validation before the Certificate expires. FirstNet will renew only on the Customer's written approval (or automatically, if the Service Schedule says the Certificate renews automatically). If the Customer does not approve the renewal, the Service ends at the end of the Subscription Term and the last Certificate will expire. The Customer is responsible for the effect on its website or services of a Certificate that expires because renewal was not approved in time.

10.3 Cancellation. Because the Certificate is bought from the CA for the Subscription Term, the Customer may cancel the Service during the Subscription Term but the Charges for that Subscription Term remain payable, subject to clause 9.2. Where the Customer is a Consumer, FirstNet may charge only a reasonable cancellation penalty as allowed by section 14 of the Consumer Protection Act 68 of 2008 ("CPA") and regulation 5 of the CPA Regulations. FirstNet applies the same reasonable cancellation penalty to a Small Business Customer (clause 19.3 of the Standard Terms and Conditions).

10.4 FirstNet may end the Service on notice if FirstNet's agreement with the CA ends or the CA stops supplying the Certificate type. In that case FirstNet will, at its choice, obtain an equivalent Certificate from another CA for the rest of the Subscription Term or refund the unused part of the Charges for the Subscription Term.

11. Suspension and revocation

11.1 The CA may revoke a Certificate under its Subscriber Agreement and the Industry Requirements, including if: the Customer requests it; the Private Key is compromised or suspected to be compromised; the Customer no longer controls a domain name in the Certificate; information in the Certificate is inaccurate or misleading; the Certificate was not issued in line with the Industry Requirements; the Certificate is being misused; or the Customer breaches the Subscriber Agreement.

11.2 FirstNet may ask the CA to revoke a Certificate if:

11.2.1 the Customer asks it to do so in writing through an authorised contact;

11.2.2 FirstNet becomes aware of any event in clause 11.1; or

11.2.3 the Charges for the Certificate remain unpaid 30 (thirty) days after FirstNet has given the Customer written notice that it intends to request revocation for non-payment.

11.3 Instead of revocation for non-payment, FirstNet may decline to reissue or renew a Certificate while undisputed Charges are overdue.

11.4 After revocation or expiry, the Customer must stop using the Certificate and its Private Key and remove it from its servers. Once a Certificate has expired or been revoked, browsers will warn users or refuse to connect, and the encryption it supported will no longer be trusted.

12. Liability specifics

12.1 The limitations and exclusions of liability in the Agreement apply to the Service. These SST do not state a separate cap.

12.2 Subject to the Agreement, FirstNet is not liable for loss or damage arising from:

12.2.1 an act or omission of the CA, including a refusal to issue, a delay in validation, a revocation under clause 11.1, an outage of the CA's systems, or a decision by a browser or operating system vendor to stop trusting the CA (in which case clause 3.5 or 10.4 applies);

12.2.2 an Unmanaged installation, or any change the Customer or its hosting provider makes to its servers;

12.2.3 compromise of a Private Key that was not caused by FirstNet's breach of clause 5.4;

12.2.4 a Certificate expiring because the Customer did not approve a renewal, did not complete a DCV or did not install a replacement Certificate in time; or

12.2.5 the security of the Customer's website, servers, applications or transactions (see clause 8.4).

12.3 For a Managed installation, FirstNet will use reasonable care. Subject to the Agreement, FirstNet is liable for damage to the Customer's server configuration, software or data only to the extent caused by its failure to use reasonable care, and its liability for data loss is limited as set out in the Agreement.

12.4 Nothing in these SST limits liability that cannot be limited by law, including under the CPA where it applies.

13. Regulatory notes

13.1 Industry Requirements. Publicly trusted Certificates are governed by the Industry Requirements, which are set by the CA/Browser Forum and browser vendors, not by South African law. They change often, and FirstNet and the CA must comply with them. Clauses 3.4, 3.5 and 11 reflect this.

13.2 Cybercrimes Act. Using a Certificate for a domain or organisation that the Customer is not entitled to represent (for example to impersonate another business) may be an offence under the Cybercrimes Act 19 of 2020 and is a breach of these SST and the Acceptable Use Policy.

13.3 ECTA electronic signatures. A TLS Certificate is not an accredited authentication product or service, and does not create an advanced electronic signature, under the Electronic Communications and Transactions Act 25 of 2002 ("ECTA").

13.4 Information shared with the CA is subject to clause 8 and POPIA.

14. Changes to these terms

14.1 FirstNet may update these SST to reflect changes in the Industry Requirements, CA products or Subscriber Agreements, the law, or how FirstNet provides the Service. FirstNet will give the Customer at least 30 (thirty) days' notice of a material change by email or by publishing it at www.firstnet.co.za/legal-notices/, except where a change in the Industry Requirements takes effect sooner, in which case FirstNet will give as much notice as it reasonably can. If a material change is to the Customer's material detriment, the Customer may cancel the affected Service by notice before the change takes effect, and clause 10.3 will not apply to that cancellation.

14.2 The version number and effective date below identify this version. This version replaces "Product Terms and Conditions - SSL Certificates" (March 2015).

SSL Certificates | Version v2026.11a | Effective date: 1 November 2026

Published by FirstNet Technology Services (Pty) Ltd (registration number 2006/031608/07), 26 Augrabies Road, Waterfall Office Park, Midrand, 1686 | 0861 989 896 | support@firstnet.co.za

Published by FirstNet Technology Services (Pty) Ltd, registration number 2006/031608/07. SSL Certificates, v2026.11a. The current version of every FirstNet legal document is at www.firstnet.co.za/legal-notices/.