Natural Person Subscriber Agreement

Classification: Public

Version: 1.0

Date: 26 – July - 2026

Document Control

☐ Draft ☐Final ☐ New Version ☒ Approved

Version	Action	Reviewer	Date	Notes
0.1	Initial Draft Version	Signit	02-Mar-2026	N/A
0.2	Amended based on Auditor feedback	Signit	09-Jul-2026	N/A
0.3	Review and Sanity Check	Signit	22-Jul-2026	N/A
0.4	Legal Review and Sanity Check	Signit	23-Jul-2026	N/A
1.0	Approval	Signit	26-Jul-2026	N/A

Sign off

Role: Signit PKI Director

Name: Mohamed El Abbouri

Date: 26 – July - 2026

Signature: 

Table Of Contents

1. Definitions

The following definitions are used throughout this agreement.

"Certificate" means a public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the certification authority which issued it.

"Certificate Application" means a request to a CA for the issuance of a Certificate.

"Certification Authority" or "CA" means an authority trusted by one or more users to create, assign, suspend or revoke certificates. For purposes of this Agreement, CA refers to Signit.

"Certificate Policy" or **"CP"** means a set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. In Signit context, the Certificate Policy is combined with the Certification Practice Statement (CP/CPS) to describe both the policy requirements and the operational practices implemented by Signit. The Signit CP/CPS is published at the address https://repository.pki.signit.sa

"Certification Practice Statement" or **"CPS"** means a document, as revised from time to time, representing a statement of the practices a CA employs in issuing Certificates. In Signit context, the CPS is combined with the Certificate Policy and published as a single CP/CPS document. The Signit CP/CPS is published at the address https://repository.pki.signit.sa

"Intellectual Property Rights" means any and all now known or hereafter existing rights associated with intangible property, including, but not limited to, registered and unregistered, trademarks, trade dress, trade names, corporate names, logos, inventions, patents, patent applications, software, know-how and all other intellectual property and proprietary rights (of every kind and nature throughout the universe and however designated).

"Public Key Infrastructure" or **"PKI"** means a set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography. In the context of this agreement, PKI shall refer to the PKI operated by Signit to enable the deployment and use of Certificates issued by Signit Subordinate CAs.

"Registration Authority" or **"RA"** means any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence

does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When “RA” is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA. In the context of this Agreement, the term “RA” refers specifically to the Registration Authority function operated by Signit.

"Relying Party" means a natural or legal person that relies upon an electronic identification or a trust service. NOTE: Relying parties include parties verifying a digital signature using a public key certificate.

"Repository" An online database containing publicly disclosed PKI governance documents such as Certification Practice Statements and Certificate status information, either in the form of a CRL or an OCSP response. Signit public repository is accessible at the address at https://repository.pki.signit.sa

"Services" mean, collectively, the services offered by Signit to Subscribers in delivering digital certificate issuing and revocation services together with the related supporting functions.

“Short-term certificate” means a Certificate issued on demand with a limited validity period not exceeding 30 minutes, intended for single or short-duration use, and which is not supported by revocation mechanisms.

"Subscriber" means a natural person bound by agreement with a trust service provider to any subscriber obligations.

“Subject” means a natural person identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber. In the context of this agreement, Subject populate the certificates issued by Signit’s Subordinate CAs.

2. Notice

THESE TERMS AND CONDITIONS AFFECT YOUR LEGAL RIGHTS AND OBLIGATIONS. PLEASE READ THEM CAREFULLY BEFORE ACCEPTING.

BY ACCEPTING THESE TERMS AND CONDITIONS, THE SUBSCRIBER REPRESENTS AND CONFIRMS THAT, AS OF THE DATE OF ACCEPTANCE:

- THEY ARE OF LEGAL AGE AND LEGALLY COMPETENT UNDER APPLICABLE LAW TO ENTER INTO THIS AGREEMENT;
- THE INFORMATION PROVIDED IN CONNECTION WITH THE APPLICATION FOR A CERTIFICATE IS TRUE, ACCURATE, AND COMPLETE;
- THEY UNDERSTAND THE LEGAL EFFECT OF ELECTRONIC SIGNATURES CREATED USING THE CERTIFICATE; AND
- THEY AGREE TO COMPLY WITH ALL OBLIGATIONS SET OUT IN THIS AGREEMENT.

IN CONSIDERATION OF ACCEPTANCE OF THESE TERMS AND CONDITIONS, THE SUBSCRIBER IS ENTITLED TO USE SIGNIT'S TRUST SERVICES AS DESCRIBED HEREIN.

3. Scope

This Agreement sets out the general terms and conditions governing the trust services provided by Signit and requested by the Subscriber in connection with the issuance and use of a digital Certificate.

Signit provides such trust services in accordance with this Agreement, applicable CP/CPS and applicable legal and regulatory requirements. This Agreement governs the relationship between Signit and the Subscriber for the entire lifecycle of the Certificate, including issuance, use, suspension, and revocation.

4. General Terms

4.1. Amendments

Signit may amend this Agreement where there is a justified operational, security, compliance, or legal need. The current version is made available at https://repository.pki.signit.sa. Material changes may be communicated via channels defined in the CP/CPS or repository notices.

4.2. Right to Refuse / Suspend

Signit may refuse, suspend, or terminate Services or Certificate Lifecycle actions if the Subscriber fails to meet the applicable identification procedures, breaches this Agreement, or where necessary for security or legal reasons.

4.3. Fees

The Subscribers shall pay the fees for the service offered.

5. Services Provided by Signit

Upon accepting this Agreement and meeting any relevant payment obligations, Signit offers the following Services:

5.1. Certificate Status Services

- CRLs for Certificates containing CDP extensions (not applicable for Short-term certificates)
- OCSP responses for Certificates containing AIA extensions.

5.2. Certificate Issuance

The Subscriber can proceed to apply for the following certification services provided by Signit:

- Issuance of Short-Term high assurance signing certificates to a natural person.

5.3. Remote Signing Service

Where remote signing services are provided:

- The private key associated with the Subscriber's Certificate is generated within certified Hardware Security Modules (HSMs) operated and controlled by Signit.
- The private key is stored securely in encrypted form and is used only within the secure cryptographic boundary of the HSM.
- Signature operations are performed using secure sole control mechanisms that require strong authentication of the Subscriber.
- The Subscriber acknowledges that in a remote signing model, the private key remains under Signit's operational control within the HSM, and signature authorization is granted only upon successful authentication of the Subscriber.

5.4. Publishing relevant agreements, policies, and practice statements

Signit publishes Information about its Certification Authorities (i.e., CAs) Certificates, CRLs/CARLs and applicable CP/CPS documents on a repository that is publicly accessible at https://repository.pki.signit.sa. Signit also publishes other relevant documents, and agreements (e.g., Subscriber Agreements and Relying Party agreements etc.) on the same repository.

5.5. Timestamping

Signit offers a non-chargeable TSA service to timestamp the document's digital signatures. Signit reserves the right to withdraw the service or charge additional fees for the service depending on the business need.

5.6. Helpdesk / Certificate Problem Reporting

Subscribers may report suspected compromise, misuse, or certificate-related incidents at any time via: **cert.problem@signit.sa**

6. Contact information

Signit POLICY ADMINISTRATION
8479 Al Mashaf, Ar Rabie Dist, Riyadh 13316
Kingdom of Saudi Arabia
Email: cert.info@signit.sa

7. Subscriber Representation and Obligations

The Subscriber represents, warrants, and undertakes that the following statements are true, accurate, and complete as of the date of acceptance of this Agreement and shall remain true throughout the lifecycle of any Certificate issued under this Agreement:

7.1. General Representations and Compliance

The Subscriber accepts and agrees to comply with this Agreement, applicable CP/CPS and all applicable laws and regulations.
The Subscriber represents and warrants that:

- they are legally competent and eligible to apply for, receive, and use Certificates and related trust services;

- they are not subject to any legal, regulatory, judicial, or contractual restriction that would prevent or limit compliance with this Agreement or applicable laws;
- all actions taken in connection with the Certificate are lawful and authorized.

7.2. Accuracy and Integrity of Information

The Subscriber shall provide information and documentation to Signit that is true, accurate, complete, and not misleading in connection with the application, issuance, use, renewal, suspension, or revocation of any Certificate.
The Subscriber shall promptly notify Signit of any change affecting the accuracy, validity, or completeness of information previously provided.
Failure to provide accurate or updated information may result in revocation of the Certificate.

7.3. Certificate Acceptance

For S hort-term C ertificates, acceptance is immediate and implicit upon issuance and first cryptographic use. Such Certificates are issued on demand for limited validity and intended for single or short-duration use.

7.4. Certificate Usage

The Subscriber shall use any Certificate solely for the purposes permitted under this Agreement, applicable CP/CPS and applicable law.
Certificates issued under this Agreement are personal to the Subscriber and shall not be transferred, assigned, shared, or otherwise made available to any other person.
The Subscriber shall immediately cease using a Certificate upon its expiration, or revocation.

7.5. Responsibility for Signed Content

The Subscriber is solely responsible for the content, legality, and consequences of any data, document, or transaction to which a digital signature or other trust service is applied using a Certificate issued under this Agreement.
Signit does not review, monitor, or validate the content of signed materials.

7.6. Protection of Private Keys and Credentials

The Subscriber shall implement appropriate measures to protect:

- any Private Key under their control (where locally stored); and

- all authentication credentials, activation data, and access mechanisms (including usernames, passwords, PINs, OTPs, or tokens) used to access or authorize use of a Certificate or remote signing service.

The Subscriber acknowledges that compromise of the authentication credentials may enable unauthorized use of the Certificate.

Any signature created using the Subscriber's private key or authentication credentials shall be presumed to have been authorized by the Subscriber unless Signit has been notified of compromise without undue delay.

7.7. Responsiveness

The Subscriber shall promptly notify Signit of any known or suspected compromise of a Private Key, activation data, or unauthorized or improper use of a Certificate. The Subscriber shall respond to Signit's instructions concerning any Private Key(s) compromise within 24 hours, including during non-business hours. If a force majeure event prevents the Subscriber from responding within this period, the Subscriber shall notify Signit and provide supporting documentation as soon as reasonably practicable.

7.8. Notification and revocation

Short-term certificates are issued with a limited validity period (i.e 30 minutes) and are not supported by revocation mechanisms due to their intended short duration and controlled lifecycle.

7.9. Permission to publish Information

The Subscriber authorizes Signit to publish the Certificate serial number, validity status, and other non-personal information necessary to enable verification of Certificate status through Certificate Revocation Lists (CRL) and Online Certificate Status Protocol (OCSP) services.
Such publication is necessary for the proper functioning and reliability of the trust service.

8. Warranties

Signit operates its Trust Services on a twenty-four (24) hour per day, seven (7) day per week basis, subject to scheduled maintenance, emergency maintenance, and events beyond its reasonable control.

Signit maintains an annual service availability target of 99.6% for its public repository and certificate status services (including CRL and OCSP services). This corresponds to a maximum cumulative downtime of approximately one (1) day and eleven (11) hours per calendar year. This availability target constitutes an operational objective and shall not be interpreted as a guarantee of uninterrupted, continuous, or error-free service.

Signit shall perform its Trust Services in accordance with this Agreement, the applicable CP and CPS, and relevant legal and regulatory requirements.

In the event that Signit discontinues any Trust Service, Signit shall:

- provide notice to affected Subscribers and other relevant parties, where applicable;
- comply with applicable legal and regulatory obligations;
- preserve and maintain relevant records and documentation in accordance with the CPS and retention requirements.

Nothing in this section shall be construed as creating a warranty of uninterrupted operation or absolute availability of the Services.

9. Liability and Indemnification

The Subscriber is solely responsible for the lawful and authorized use of any Certificate or Trust Service issued under this Agreement and for compliance with the obligations set out herein.
The Subscriber shall indemnify and hold harmless Signit, its officers, employees, contractors, and agents from and against any claims, actions, losses, liabilities, damages, and reasonable costs (including legal fees) arising out of or directly related to:

a) any misuse, unauthorized use, or improper use of a Certificate attributable to the Subscriber;
b) any material breach of this Agreement or the applicable CP/CPS by the Subscriber; or
c) any unlawful, fraudulent, or negligent act or omission by the Subscriber in connection with the use of Signit's Trust Services or Certificates.

The Subscriber's indemnification obligations shall not apply to the extent that a claim arises directly from Signit's gross negligence, willful misconduct, or material breach of its obligations under this Agreement.
Nothing in this section shall exclude or limit liability where such exclusion or limitation is prohibited by applicable law.

Liability. Signit's total liability for all claims arising from or related to the Services shall not exceed the amounts paid to Signit during the twelve months immediately preceding the date of the claim.

10. Disclaimer of Warranty

To the maximum extent permitted by applicable law, Signit shall not be held liable, except in cases of fraud or deliberate abuse, for:

- any loss of profit, loss of business, or loss of anticipated savings;
- any loss of data or corruption of data, except where such loss results directly from Signit's gross negligence or willful misconduct;
- any indirect, incidental, or consequential damages arising out of or related to the use, provisioning, issuance, suspension, revocation, or non-issuance of Certificates or digital signatures;
- any liability arising where an error in verified information is the result of fraud, willful misconduct, negligence, or intent to deceive by the Subscriber, its Authorized Representatives, or any other person acting on behalf of the Subscriber, or by any person relying on the Certificate;
- any liability arising from the Subscriber's violation of applicable laws or regulations in the Kingdom of Saudi Arabia, including laws relating to intellectual property, malicious code, or unauthorized access to computer systems; or
- any failure to perform obligations under this Agreement where such failure results from force majeure events, including but not limited to natural disasters, governmental actions, or network or system failures beyond Signit's reasonable control.

Nothing in this section shall limit or exclude the Subscriber's liability or indemnification obligations under this Agreement.

11. Privacy and Data Protection

Signit processes personal data in accordance with applicable data protection laws and regulations.
Access to personal data is restricted to authorized and trusted Signit personnel who require such access strictly for legitimate purposes including certificate lifecycle management, trust service delivery, security operations, compliance, audit, and incident handling.

Signit collects, uses, retains, and discloses personal data in a lawful, fair, transparent, and proportionate manner, and in compliance with applicable privacy, personal data protection, and, where applicable, confidentiality and trade secret laws.
Personal data may be disclosed to third parties only:

- where necessary for the provision, validation, or status checking of Certificates or related trust services;
- where disclosure is required by applicable law, regulation, judicial order, or competent authority;
- where the data subject has provided explicit consent; or
- where disclosure is necessary to protect the integrity, security, or reliability of the trust service.

Where personal data is disclosed pursuant to a legal obligation or authorized request, Signit shall implement reasonable technical and organizational measures to ensure that such data is used solely for the purposes for which it was disclosed.
Signit implements appropriate technical and organizational security measures designed to protect personal data against unauthorized access, alteration, disclosure, loss, or destruction, and to preserve the confidentiality, integrity, and availability of information processed within its Trust Services.
Nothing in this section shall require Signit to disclose information that it is legally prohibited from disclosing.

12. Confidentiality

The Subscriber shall treat as confidential and shall not disclose, publish, or use, except as necessary for the performance of this Agreement, any non-public operational, security, technical, procedural, commercial, or proprietary information relating to Signit's Trust Services that is disclosed or made available to the Subscriber in connection with this Agreement ("Confidential Information").

The Subscriber shall take reasonable measures, appropriate to their circumstances, to protect Confidential Information against unauthorized access, disclosure, or misuse.

The obligations set forth in this Section shall not apply to information that:

- is or becomes publicly available without breach of this Agreement;
- was lawfully known to the Subscriber prior to disclosure;
- is independently developed without reference to the Confidential Information; or
- is required to be disclosed by applicable law, CP/CPS, regulation, court order, or competent authority, provided that the Subscriber gives prior notice to Signit where legally permitted.

The confidentiality obligations under this Section shall survive the termination or expiration of this Agreement for so long as the information remains non-public.

13. Retention Period

Signit, acting as a Trust Service Provider (TSP), maintains internal records and ensures archival in accordance with the applicable CP/CPS for a period of ten (10) years following the expiration of any Certificate, including documentation related to the security of Certification Authority systems and the verification, issuance, and revocation of Certificates.

14. Term and Termination

This Agreement shall remain in force from the date of acceptance until the expiration or revocation of the Certificate issued to the Subscriber, unless terminated earlier in accordance with this Section.

The Subscriber may terminate this Agreement at any time by requesting revocation of the Certificate.

Signit may revoke, or terminate the Certificate and/or related Trust Services, with immediate effect where necessary, including in the event of:

- suspected or confirmed security compromise;
- compromise of a Private Key or authentication credentials;
- material breach of this Agreement by the Subscriber;
- misuse or unauthorized use of the Certificate;
- provision of inaccurate or misleading information by the Subscriber;
- legal or regulatory requirement; or
- circumstances that materially threaten the integrity, security, or reliability of the Trust Services.

Termination or revocation of a Certificate shall not affect any rights, obligations, or liabilities that accrued prior to termination.

15. Miscellaneous Provisions

15.1. Interpretation and Precedence

In the event of any conflict or inconsistency between this Relying Party Agreement and the applicable CP/CPS, the terms of this Agreement shall prevail with respect to the contractual rights and obligations of the Parties, while the CP/CPS shall continue to govern the technical, operational, and security requirements relating to the issuance,

management, validation, suspension, and revocation of Certificates, unless this Agreement expressly provides otherwise.

15.2. Governing Laws

The laws of the Kingdom of Saudi Arabia shall govern the enforceability, construction, interpretation, and validity of the present agreement.

15.3. Entire Agreement

This Agreement, together with the documents incorporated by reference herein (including the applicable CP/CPS), constitutes the entire agreement between the parties and supersedes all prior understandings, oral or written, between the parties.

15.4. Dispute Resolution

Any dispute, controversy, or claim arising out of or in connection with this Agreement, the applicable CP/CPS, or the services provided by Signit shall first be referred to Signit's Legal Department for good faith discussions with a view to resolving the dispute amicably. If the dispute is not resolved within thirty (30) days from the date on which written notice of the dispute is received by Signit, either Party may refer the dispute to the competent courts of the Kingdom of Saudi Arabia, which shall have exclusive jurisdiction.

15.5. Severability

If any provision of this Agreement, or the application thereof, shall for any reason and to any extent, be invalid or unenforceable, the remainder of this Agreement and application of such provision to other persons or circumstances shall be interpreted so as best to reasonably effect the intent of the parties hereto.

15.6. Force Majeure

Signit shall not be liable for any losses, costs, expenses, liabilities, damages, or claims arising out of or related to delays in performance or from failure to perform its obligations if such failure or delay is due to circumstances beyond Signit’s reasonable control, including without limitation, acts of any governmental body, war, insurrection, sabotage, embargo, fire, flood, strike or other, interruption of or delay in transportation, unavailability of, interruption or delay in telecommunications or third party services.

— End of Document —