

Legal Person Subscriber Agreement

Classification: Public

Version: 1.0

Date: 26-Jul-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 Based on Signit Comments	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	4
2. Notice	6
3. Scope	6
4. General Terms	6
4.1. Amendments	6
4.2. Right to Refuse / Suspend	6
4.3. Fees	6
5. Services Provided by Signit	7
5.1. Certificate Status Services	7
5.2. Certificate Issuance	7
5.3. Remote Sealing Service	7
5.4. Publishing relevant agreements, policies, and practice statements	7
5.5. Timestamping	7
5.6. Helpdesk / Certificate Problem Reporting	8
6. Contact information	8
7. Subscriber Representation and Obligations	8
7.1. Legal Capacity and Authority	8
7.2. Authorized Representatives	8
7.3. Accuracy and Integrity of Information	9
7.4. Certificate Acceptance	9
7.5. Certificate Usage	10
7.6. Responsibility for Sealed Content	10
7.7. Protection of Credentials	11
7.8. Responsiveness	11
7.9. Notification and revocation	12
7.10. Permission to publish Information	12
8. Warranties	14
9. Liability and Indemnification	14
10. Disclaimer of Warranty	15
11. Privacy and Data Protection	16
12. Confidentiality	16

13.	Retention Period.....	17
14.	Term and Termination.....	17
15.	Miscellaneous Provisions.....	18
15.1.	Interpretation and Precedence.....	18
15.2.	Governing Laws.....	18
15.3.	Entire Agreement.....	18
15.4.	Dispute Resolution.....	19
15.5.	Severability.....	19
15.6.	Force Majeure	19

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-forgable 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/>

"eSeal Certificate" A certificate issued to a legal person to authenticate electronic documents or transactions on behalf of that entity.

"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.

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

"Subject" means a legal person identified in a Certificate as the Subject. In the context of this agreement, Subject populates the certificates issued by Signit's Legal Person Subordinate CA.

2. Notice

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

BY ACCEPTING THIS AGREEMENT, THE SUBSCRIBER REPRESENTS AND WARRANTS THAT:

1. IT HAS FULL LEGAL CAPACITY AND AUTHORITY TO ENTER INTO THIS AGREEMENT.
2. THE INDIVIDUAL ACCEPTING THIS AGREEMENT IS DULY AUTHORIZED TO BIND THE SUBSCRIBER; AND
3. THE SUBSCRIBER WILL COMPLY WITH THIS AGREEMENT AND THE APPLICABLE CP/CPS

3. Scope

This Agreement governs the contractual relationship between Signit and the Subscriber for the provision and use of the Services and any Certificates issued to the Subscriber.

This Agreement is intended to operate together with the Signit CP/CPS.

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. Fees are defined in the contractual/financial agreement.

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
- 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:

- Electronic Seal issued to a legal person

5.3. Remote Sealing Service

- Key pairs associated with remote sealing are generated and stored throughout their lifecycle within HSMs operated and controlled by Signit, on Signit premises, as described in the CP/CPS.
- Private keys are not exported from HSM.
- Sealing operations are authorized using strong authentication and sole-control mechanisms applied to Authorized Representatives.

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 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 undertakes that the following obligations apply throughout the lifecycle of any Certificate issued under this Agreement:

7.1. Legal Capacity and Authority

The Subscriber represents and warrants that it is a duly constituted legal person, validly existing under applicable law, and has full legal capacity and authority to enter into this Agreement and to apply for, receive, and use Certificates and trust services provided by Signit.

The Subscriber represents and warrants that all actions performed under this Agreement are carried out in accordance with its constitutional documents, internal governance rules, and applicable laws, and that it is not subject to any legal, regulatory, judicial, or contractual restriction that would prevent compliance with this Agreement or the applicable CPS.

7.2. Authorized Representatives

The Subscriber shall designate one or more natural persons as Authorized Representatives to act on its behalf in connection with the application, issuance, activation, management, use, suspension, and revocation of Certificates.

Authorized Representatives act solely as agents of the Subscriber and shall not become parties to this Agreement. The Subscriber represents and warrants that each Authorized Representative is duly authorized under its constitutional documents, internal governance rules, and applicable law to perform the actions assigned to them.

The Subscriber shall ensure that the authority granted to each Authorized Representative is clearly defined, documented, and kept up to date.

Any act or omission of an Authorized Representative in connection with a Certificate or related service shall be deemed an act or omission of the Subscriber, whether such act or omission was authorized internally or exceeded internal limitations, provided it was performed using the access rights or credentials granted by or attributable to the Subscriber.

The Subscriber remains fully responsible for the supervision, control, and actions of its Authorized Representatives to the extent permitted by applicable law.

7.3. Accuracy and Integrity of Information

The Subscriber shall ensure that all information and documentation submitted to Signit in connection with the application, issuance, renewal, modification, suspension, or revocation of any Certificate is true, accurate, complete, and not misleading at the time of submission.

The Subscriber shall promptly notify Signit, without undue delay, of any change that may affect the accuracy, validity, or completeness of information previously provided, including but not limited to:

- changes in the Subscriber's legal name, legal form, registration status, or corporate existence;
- changes in authorized signatories or Authorized Representatives;
- withdrawal or limitation of authority of any Authorized Representative;
- any circumstance that may affect the reliability of the Certificate.

The Subscriber acknowledges that Signit relies on the information provided by the Subscriber for certificate issuance and lifecycle management, and that failure to provide accurate or updated information may result in revocation of the Certificate in accordance with this Agreement and Signit CP/CPS.

7.4. Certificate Acceptance

Upon issuance and making the Certificate available to the Subscriber, the Subscriber shall promptly review the Certificate to verify the accuracy of all information contained therein.

If the Subscriber does not notify Signit in writing of any objection or request revocation within twenty-four (24) hours from the time the Certificate is made available, the Certificate shall be deemed accepted.

Acceptance of the Certificate confirms that:

- the information contained in the Certificate is accurate and complete;
- the Certificate corresponds to the Subscriber's request;
- the Subscriber agrees to use the Certificate in accordance with this Agreement and the applicable CP/CPS.

For the avoidance of doubt, any use of the Certificate, including activation or use of remote sealing functionality, shall constitute irrevocable acceptance of the Certificate.

7.5. Certificate Usage

The Subscriber shall use any Certificate issued by Signit solely for the purposes and usages permitted under this Agreement and the applicable CP/CPS, and in compliance with all applicable laws and regulations.

Where an eSeal Certificate is issued for use within Signit's remote sealing service, the Subscriber shall ensure that the Certificate is used exclusively through approved applications, systems, or integrations authorized by Signit and in accordance with the security controls defined in the CP/CPS.

The Subscriber shall not:

- use an eSeal Certificate for personal identification purposes;
- use an eSeal Certificate to create electronic signatures attributable to a natural person;
- use the Certificate for any purpose other than those expressly permitted under the CP/CPS;
- attempt to circumvent, bypass, or interfere with Signit's technical or security controls.

Certificates issued under this Agreement are non-transferable. The Subscriber shall not assign, sublicense, or otherwise make a Certificate available to any third party, except through Authorized Representatives acting strictly within the scope of their authority and under the control of the Subscriber.

The Subscriber remains responsible for all uses of the Certificate carried out through credentials, access rights, or systems under its control.

7.6. Responsibility for Sealed Content

The Subscriber is solely responsible for the content, lawfulness, accuracy, authorization, and consequences of any data, document, or transaction to which an electronic seal is applied using a Signit remote sealing service provided under this Agreement.

Signit does not review, approve, or validate the content of sealed materials, except to the extent required by applicable law or necessary for the operation and security of the Trust Services.

The application of an electronic seal confirms the origin and integrity of the sealed data in accordance with the applicable Certificate policy and practices statement but does not constitute Signit's approval, endorsement, or confirmation of the legality, accuracy, or validity of the sealed content or underlying transaction.

7.7. Protection of Credentials

The Subscriber shall implement appropriate technical and organizational measures to safeguard all authentication credentials, activation data, and access mechanisms (including usernames, passwords, PINs, OTPs, or similar authentication factors) used to access, activate, or authorize the use of a Certificate or remote sealing service.

The Subscriber shall ensure that such credentials:

- are kept confidential and not disclosed to unauthorized persons;
- are protected against loss, theft, misuse, or unauthorized access.

The Subscriber acknowledges that compromise or misuse of such credentials may enable unauthorized use of the Certificate or sealing functionality. Any use of the Certificate or remote sealing service performed using credentials issued to or attributable to the Subscriber shall be deemed authorized by the Subscriber, unless the Subscriber has notified Signit of the compromise without undue delay in accordance with this Agreement. The Subscriber shall immediately notify Signit upon becoming aware of any actual or suspected compromise, loss, misuse, or unauthorized disclosure of authentication credentials.

The Subscriber bears responsibility for the consequences of failure to adequately protect such credentials, to the extent permitted by applicable law.

7.8. Responsiveness

The Subscriber shall provide, without undue delay, any information reasonably requested by Signit in connection with a known or suspected compromise, misuse, or unauthorized use of:

- a Certificate;
- authentication credentials or access rights;
- an Authorized Representative's account; or
- any mechanism used to authorize remote sealing operations.

The Subscriber shall respond to Signit's security-related requests and instructions within twenty-four (24) hours, including during non-business hours where the matter may affect the security or reliability of the Certificate or remote sealing service.

Where a force majeure event prevents the Subscriber from responding within this period, the Subscriber shall document the circumstances and notify Signit without undue delay once communication becomes reasonably possible.

Any known or suspected compromise of a private key held within Signit's remote sealing infrastructure shall be investigated and managed by Signit in accordance with the applicable CP/CPS and incident-management procedures.

7.9. Notification and revocation

The Subscriber shall immediately cease use of the Certificate and, where applicable, suspend any use of remote sealing functionality, and shall request revocation of the Certificate without undue delay if any of the following circumstances occurs:

- the Subscriber becomes aware of, or reasonably suspects, compromise, misuse, or unauthorized access relating to the Certificate, associated authentication credentials, or remote sealing authorization mechanisms;
- the Subscriber breaches a material obligation under this Agreement or the applicable CP/CPS that affects the reliability of the Certificate;
- any information relating to the Subject contained in the Certificate becomes inaccurate, misleading, or invalid;
- the authority of an Authorized Representative is withdrawn or limited in a manner affecting certificate use;
- this Agreement is terminated;
- use of the Certificate is no longer authorized; or
- any circumstance arises that materially threatens the security, integrity, or reliability of the Certificate.

Where remote sealing services are provided, the Subscriber acknowledges that the private key remains under the control of Signit within certified HSMs. Accordingly, the Subscriber's obligation to cease use applies to the suspension of authorization or access to sealing operations.

Failure to notify Signit without undue delay may result in continued reliance on the Certificate by third parties, and the Subscriber may bear responsibility for consequences arising from such delay to the extent permitted by applicable law.

Signit reserves the right to revoke a Certificate where required under the CP/CPS, applicable law, or where necessary to protect the integrity of the offered service.

7.10. Permission to publish Information

The Subscriber acknowledges and expressly authorizes Signit to publish and make available information relating to the Certificate as necessary for the proper operation of the trust service, including but not limited to:

- the Certificate itself (where applicable);
- the Certificate serial number;
- Certificate status information (valid, suspended, revoked);
- revocation data through Certificate Revocation Lists (CRL);
- status information through Online Certificate Status Protocol (OCSP) services;
- any other non-personal information required to enable Relying Parties to verify the validity and status of the Certificate.

Such publication shall be carried out in accordance with applicable law, the CP/CPS, and through the Signit Repository and validation service.

The Subscriber acknowledges that publication of status information is an essential component of the trust service and is necessary to ensure reliability and legal effect of Certificates.

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. The stated downtime represents the total downtime over the calendar year and should not be interpreted as the maximum duration of a single service interruption. Signit will make reasonable efforts to restore the affected service as soon as practicable following any unplanned interruption. 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, as a Legal Person, is solely responsible for the lawful and authorized use of any Certificate and related Trust Services issued under this Agreement, in accordance with the representations and obligations set out herein.

The Subscriber shall indemnify, defend, and hold harmless Signit, its officers, directors, employees, contractors, and agents from and against any and all claims, actions, demands, damages, losses, liabilities, costs, and expenses (including reasonable legal fees and expenses) arising out of or related to:

- a) any misuse, unauthorized use, or improper use of a Certificate or Trust Service attributable to the Subscriber;
- b) any breach by the Subscriber of this Agreement;

- c) any inaccurate, misleading, or incomplete information provided by the Subscriber;
- d) any unlawful, fraudulent, or negligent act or omission by the Subscriber or its Authorized Representatives, employees, officers, agents, or systems in connection with the use of Certificates or Trust Services;
- e) any use of a Certificate or remote sealing functionality performed using authentication credentials issued to or attributable to the Subscriber.

The Subscriber's indemnification obligations shall not apply to the extent that a claim, loss, or damage arises directly from Signit's gross negligence, willful misconduct, or material breach of its obligations under this Agreement.

Nothing in this section shall limit any other rights or remedies available to Signit under this Agreement or 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 other proprietary information relating to Signit's Trust Services that is disclosed or made available to the Subscriber in connection with this Agreement ("Confidential Information").

Confidential Information includes, without limitation:

- security architecture or control mechanisms;
- technical integration details;
- audit-related information;

- non-public policies, reports, or documentation.

The Subscriber shall implement reasonable measures to protect Confidential Information against unauthorized access, disclosure, or misuse and shall ensure that such information is disclosed only to persons who have a legitimate need to know and who are bound by confidentiality obligations no less restrictive than those set out herein.

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, regulation, or competent authority, provided that the Subscriber gives prior notice to Signit where legally permitted.

The confidentiality obligations set out in this Section shall survive the termination or expiration of this Agreement.

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

14.1 This Agreement takes effect on the date the Subscriber accepts it and shall remain in force until the expiration or revocation of the Certificate issued to the Subscriber, unless terminated earlier in accordance with this Section.

14.2 Termination by the Subscriber. The Subscriber may terminate this Agreement at any time by requesting revocation of the Certificate and ceasing all use of the Certificate and, where applicable, the remote sealing service.

14.3 Suspension, blocking, revocation and termination by Signit. Without prejudice to any other right or remedy available under this Agreement or the applicable CP/CPS, Signit may suspend, block, revoke, or terminate the Certificate and/or the related Trust Services, with immediate effect where necessary, including in the event of:

- (a) suspected or confirmed security compromise; or
- (b) compromise of a Private Key, activation data, or authentication credentials; or
- (c) material breach of this Agreement or the applicable CP/CPS by the Subscriber; or
- (d) misuse or unauthorized use of the Certificate or remote sealing functionality; or

- (e) provision of inaccurate, misleading, or incomplete information by the Subscriber; or
- (f) withdrawal or limitation of the authority of an Authorized Representative in a manner affecting certificate use; or
- (g) any legal or regulatory requirement; or
- (h) any circumstance that materially threatens the integrity, security, or reliability of the Trust Services.

14.4 Survival. Termination, expiration, suspension, or revocation of the Certificate or of this Agreement shall not affect any rights, obligations, or liabilities that accrued prior to the effective date of termination, and shall not relieve the Subscriber of any payment, indemnification, confidentiality, or other obligation that is expressed to survive or that by its nature is intended to survive. Without limitation, Sections 9 (Liability and Indemnification), 10 (Disclaimer of Warranty), 11 (Privacy and Data Protection), 12 (Confidentiality), 13 (Retention Period), and 15 (Miscellaneous Provisions) shall survive the termination or expiration of this Agreement.

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 —