Relying Party 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 in the document "Report of Findings and Recommendations for Signit, the Kingdom of Saudi Arabia, version 2 as of 2026-05-03"	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

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.

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

“**Subject**” means a natural person, device, system, unit, or Legal Entity 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 Subordinate CAs depending on the type of certificates.

.

2. Notice

YOU MUST READ THIS RELYING PARTY AGREEMENT ("AGREEMENT") BEFORE RELYING ON ANY IDENTITY INFORMATION IN A SIGNIT ISSUED CERTIFICATE, VALIDATING A SIGNIT ISSUED CERTIFICATE, USING A SIGNIT DATABASE OF CERTIFICATE REVOCATIONS, OR RELYING ON ANY SIGNIT CERTIFICATE-RELATED INFORMATION (COLLECTIVELY, " SIGNIT INFORMATION").

IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT SUBMIT A QUERY AND DO NOT DOWNLOAD, ACCESS, OR RELY ON ANY SIGNIT INFORMATION.

IN CONSIDERATION OF YOUR AGREEMENT TO THESE TERMS, YOU ARE ENTITLED TO USE SIGNIT INFORMATION AS SET FORTH HEREIN.

3. Scope

This relying party Agreement ("this Agreement") controls the use of information provided by Signit:

- As a result of a search for a digital certificate,
- The verification of the status of digital signatures created with a private key corresponding to a public key certificate issued by Signit ("the certificate validation"),
- Information published on Signit website < https://repository.pki.signit.sa/ >
- Any services advertised or exposed through the Signit website < https://repository.pki.signit.sa/ >

This Agreement is published on Signit's repository and is deemed accepted by, and becomes effective between, Signit and the Relying Party when the latter submits a certificate validation query or otherwise relies on information provided by Signit through its repository or certificate validation services.

This Agreement does not apply to information provided in or used from demo, free, and test certificates.

4. Signit Obligations

Signit shall use commercially reasonable efforts to ensure the accuracy of the information it verifies and includes in Certificates, in accordance with the applicable CP/CPS.

Signit shall make every reasonable effort to ensure that the information contained in its Certificates is valid and accurate, acknowledging the trusted position it holds.

Signit shall take all reasonable steps to ensure that the information contained in its records and directories is accurate, complete, and updated in a timely manner.

5. Relying Party Obligations

The Relying Party acknowledges that they have adequate information to decide whether to rely upon the information provided in certificates issued by Signit.

The Relying Party shall:

(i) Use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension),
(ii) Verify the validity by ensuring that the certificate has not expired,
(iii) Establish trust in the CA who issued a certificate by verifying the certificate path in accordance with the guidelines set by the RFC 5280,
(iv) Ensure that the certificate has not been revoked by accessing current revocation status information available at the locations specified in the certificate to be relied upon,
(v) Determine that such certificate provides adequate assurances for its intended use,
(vi) Use the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations to be performed, as a condition of relying on a Certificate in connection with each such operation.

Specifically, when relying on a timestamp token, the relying party shall:

1. Verify that the timestamp token (TST) has been correctly signed and that the private key used to sign the timestamp has not been compromised until the time of the verification
2. Consider any limitations on the usage of the timestamp indicated by the TSA-PS and the CP/CPS published at < https://repository.pki.signit.sa/ >
3. In case the verification takes place after expiry of the timestamp certificate, the relying party should consider the following (taken from guidance denoted in Annex D of ETSI EN 319 421):
    a. Verify that the TSU certificate had not been revoked at the relevant time, and
    b. Verify that the cryptographic hash function and the signing algorithm used in the timestamp token are still considered secure.

The Relying Party is solely responsible for deciding whether to rely on the information provided by Signit.

The Relying Party bears sole responsibility for any indirect damages it suffers as a result of its decision to rely on information provided by Signit

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.

6. Disclaimer of Warranty

Within the scope of the law of the Kingdom of Saudi Arabia, and except in the case of fraud, or deliberate abuse, Signit cannot be held liable for:

- The accuracy of any information contained in certificates except as it is warranted by the subscriber that is the party responsible for the ultimate correctness and accuracy of all data transmitted to Signit with the intention to be included in a CA certificate,
- Indirect damage that is the consequence of or related to the use, provisioning, issuance or non-issuance of certificates or digital signatures,
- Wilful misconduct of any third-party participant breaking any applicable laws in the Kingdom of Saudi Arabia, including, but not limited to those related to intellectual property protection, malicious software, and unlawful access to computer systems,
- For any damages suffered whether directly or indirectly because of an uncontrollable disruption of the Signit’s services,
- Any form of misrepresentation of information by the subscribers or relying parties on information contained in the CP/CPS or any other documentation made public by the Signit and related to the Signit services.

.

7. Miscellaneous Provisions

7.1 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.

7.2 Governing Laws

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

7.3 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.

7.4 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.

7.5 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.

7.6 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 —