DIGITAL SIGNING POLICY

Document Classification:

Public

Version Number : 1.1

Issue Date: 2 December, 2020

Table of Contents

1. POLICY STRUCTURE AND DEFINITIONS

1.1 POLICY STRUCTURE

This policy document contains the following elements:

- **Purpose:** This section clearly states the purpose of the policy with regards to NCDC Digital Signing Policy.
- **Scope: T**his section defines various internal and external entities as well as the people to which a particular policy statement applies.
- **Policy:** This section describes the policy statement of NCDC Digital Signing Policy.
- **Related NCDC Documents:** This section mentions other policies, procedures, forms etc., which can be referred to along with this policy document.
- **Compliance:** This section contains a statement that NCDC policies will be complied with and that violations may result in disciplinary action.
- **Waiver Criteria:** This section provides a formal process for obtaining approval for a waiver to a policy. Waivers should only be used in exceptional situations when communicating non-compliance with the policy for a specific period of time.
- **Executor(s):** The person / department responsible for implementation of this policy.
- **ISO27001:2013 Control References:** This section provides references to the security controls that have been used in this policy.

1.2 DEFINITIONS

The terms used in this document shall have the meanings as defined in the NCDC Glossary which can be found at https://www.ncdc.gov.sa.

2. PURPOSE

The objective of the document is to define a signature policy that is expressing both the conformity of electronic signatures created by Trust Service Providers, and the validity of such electronic signatures when verified by relying parties.

As stated in the introduction of [TS 119 172-1], “the purpose of a signature policy is to describe the requirements imposed on or committing the involved actors (signers, verifiers, relying parties and/or potentially one or more Trust Service Providers) with respect to the application of signatures to documents and data that will be signed in a particular context, transaction, process, business or application domain, in order for these signatures to be considered as valid or conformant signatures under this signature policy.”

The present signature policy defines applicability rules, that is a “set of rules, applicable to one or more digital signatures, that defines the requirements for their determination of whether a signature is fit for a particular business or legal purpose”.

The present document is based on 2 levels of electronic signatures (advanced and qualified) using PKI-based digital signatures are defined. The applicability that is targeted in the present document is the determination whether a digital signature is of one of these two levels.

- Advanced level ("advanced electronic signature"): Advanced Electronic Signatures benefitting from a stronger legal effect, as long as:
    - it is uniquely linked to the signatory;
    - it is capable of identifying the signatory;
    - it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
    - it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

- Qualified level ("qualified signature"): Built on top of the Advanced level, with stronger requirements on the signing certificate and the protection of the private key. Among other requirements, this involves a stricter authentication of the signatory (e.g. via face-to-face or equivalent) and a higher protection of the private key (e.g. via hardware). A signature created by a private key whose signing certificate is of level of assurance High, is recognized as being at the qualified level.

3. SCOPE

The signature policy defined in the present document is suitable for a large range of business or application domains: B2B, B2C, G2B, G2C, etc.

It is however limited to electronic transactions in KSA, governed by the e-Transactions Law.

4. POLICY

The present policy focuses on the PKI-based digital signatures provided by Trust Service Providers, it is vital that the following shall be followed:

- Trust Service Provider shall implement set of policy and security practices recommended by NCDC.

- Subscriber shall obtain suitable digital signature certificate from approved Trust Service Provider under the Saudi National PKI.

- In order to cover document signing and transaction signing needs , minimum set of accepted formats shall be PDF, XML, MS Word, Emails (S/MIME).

- In terms of scope/range of the signature, the signature shall cover whole data (meaning the whole document or the whole transaction).

- The signature format supported shall be either PAdES, XAdES or PKCS#7.

- The Trust Service Provider shall augment the signature up to the timestamp level at the time of creation.

- Approved licensed providers by NCDC can offer Timestamp as a separate service. The timestamp certificate used for the service shall be obtained from the CAs under the Saudi National PKI.

- The intention to sign of the signatory is represented by the nonrepudiation / contentCommitment key usage bit in the certificate.

- In terms of cryptographic algorithms, as described in the Saudi National PKI Policy:
    - The hashing algorithm is recommended to be SHA-256;
    - The asymmetric key algorithm is recommended to be RSA;
    - The minimum key length is recommended to be 2048 bits and
    - Any other suite of algorithms after duly approval of NCDC.

- The signer (subscriber) shall be a natural person (human entity) that is a Saudi national or resident of the Kingdom.

- The subscriber shall protect their private key and keep it secret be it stored local or centralized.

- The Trust Service Provider shall define identity verification requirements for subscriber (natural person) in a way appropriate to the Level of Assurance corresponding to certificates being requested.

- The Trust Service Provider shall incorporate appropriate OID corresponding to the Level of Assurance in the advanced, qualified signature certificates.

- Based on the assurance level; digital signature shall be either advanced or qualified offered to the natural person.

- The selection of the appropriate Level of Assurance will depend on the business context, and the signature legal level to be reached. The following table maps the Level of Assurance and the signature legal level.

Certificate Level of Assurance	Signature legal level
High	Qualified
Medium	Advanced

- The Qualified level shall be considered as the highest necessary level to reach the legal effect of handwritten signatures.

- The Legal Effects of High Level of Assurance are mentioned in Electronic Transactions Law - Chapter 4 - Article 14

- The Legal Effects of Medium Level of Assurance are mentioned in Electronic Transactions Law - Chapter 2 - Article 9

- The issuer of the certificate shall be a licensed Trust Service Provider under the Saudi National PKI. The acceptable trust anchors are the licensed Government and Commercial CAs issuing end-entity certificates under the Saudi National Root-CA.

- The Trust Service Provider shall provide subscriber disclosure that outlines the terms of conditions for using their services.

- Subscriber shall understand the terms of conditions of Trust Service Provider services before start using them.

- The end entity certificate issued to subscriber for digital signing shall comply with issuing CA CP and CPS.

- For subscribers using centralized Signing Platform, Signing keys shall be generated using FIPS 140-2 Level 3 or higher certified hardware or Software security module (based on Certificate Level of Assurance) and stored in an encrypted database on the central storage.

- Key wrapping is accepted method for the centralized Signing Platform subscribers.

- If a signer (subscriber) believes that the signer's private key was stolen or otherwise compromised, the signer shall contact Trust Service Provider for revocation of certificate.

- If the subscriber's digital signature does not appear valid, the relying party shall not trust the source of the document or correspondence.

- The Trust Service Provider shall provide time of signing (claimed signing time) based on the clock of the Trust Service Provider and not the clock of the signatory for XAdES and PAdES formats.

- For the ease of validation by a relying party, the full chain of certificates from the signing certificate up to the applicable trust anchor shall be included in the signature.

- Trust Service Provider is in charge of augmenting the signature to a signature with time. At validation, the relying party is responsible for augmenting to signature with long-term validation material, or signature providing long-term availability and integrity of validation material.

- Trust Service Provider providing trust services shall use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.

- Trust Service Providers shall comply with Saudi National PKI and other compliance requirements and ensure compliance via third party audit.

- Trust Service Providers shall gather only required information of subscriber essential for their services and comply with NCDC Privacy Policy.
- The governing law is the e-Transactions law in KSA.
- Possible conflicts shall be resolved as per the NCDC Dispute Resolution Policy.
- Queries regarding Digital Signing Policy shall be directed at:
    - Email: info@ncdc.gov.sa
    - Telephone: +966 11 452 2197

5. RELATED NCDC DOCUMENTS

- Issuing CA CP
- Issuing CA CPS
- Saudi National PKI Policy
- NCDC Dispute Resolution Policy
- NCDC Privacy Policy
- E-Transaction Law

6. COMPLIANCE

Compliance with this policy is mandatory and will be reviewed periodically by Trust Services Governance General Department. Violations of NCDC policies, standards, and procedures will result in corrective action by NCDC management. Disciplinary action will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets.
- Other actions as deemed appropriate by NCDC management, Business Support department, and Trust Services Governance General Department.

7. WAIVER CRITERIA

Requested waivers must be formally submitted to NCDC, including justification and benefits attributed to the waiver, and must be approved by NCDC Chief Executive Officer. The waiver should only be used in exceptional situations when communicating non-compliance with the policy for a specific period of time (subject to a maximum period of 1 year). At the completion of the time period the need for the waiver should be reassessed and re-approved, if necessary. No policy should be provided waiver for more than three consecutive terms. The waiver should be monitored to ensure its concurrence with the specified period of time and exception. All exceptions to this policy must be communicated through the Policy Waiver Request Form.

8. EXECUTOR(S)

The following are the executors of this policy and its associated procedure:

- Trust Services Governance General Manager
- CAs under Saudi National Root
- Trust Service Providers
- Any entity using their own signing application

9. ISO27001:2013 CONTROL REFERENCES

- A.10.1.1 - Policy on the use of cryptographic controls
- A.10.1.2 - Key management
- A.18.1.5 - Regulation of cryptographic controls