ELECTRONIC SEAL POLICY

Document Classification:

Public

Version Number : 1.0

Issue Date: December 01, 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 Electronic Seal 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 Electronic Seal 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.
- **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 this document is to define an electronic seal policy to support relying parties and end users of electronic seal services to use these services provided by Trust Service Providers.

Technical point of view, an electronic seal is based on the same procedure as the electronic signature issued by Trust Service Provider. An electronic seal is; data in electronic form attached to other data in electronic form or logically linked to such data in order to ensure the origin and integrity of the data.

The eIDAS Regulation defines an electronic seal as “data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter’s origin and integrity”. A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.

A seal is “generated” by a creator of the seal, possibly “augmented” (i.e. completed with related proofs or evidences), “validated” by the receiver of the sealed data (so-called “relying party”), and possibly preserved, in some cases for a long term.

Electronic seals are created by an electronic seal creation device, which is defined in the eIDAS Regulation as “a configured software or hardware used to create an electronic seal by means of an ‘electronic seal creation data’ (i.e. “a unique data which is used by the creator of the seal to create an electronic seal”)”.

Electronic seals in general shall not be denied legal effect and admissibility as evidence in legal proceedings. Within the electronic seal family:

- the advanced electronic seal (AdESeal) – which requires security features that ensure it is uniquely linked to the signatory, it is capable of identifying the signatory entity and it is linked to the data in such a manner that any subsequent change of the data is detectable.

- the qualified electronic seal (QESeal) – which is an advanced electronic seal which provides additional level of assurance on the identity of the creator of the seal and an enhanced protection and level of assurance on the seal creation.

The present electronic seal policy defines applicability rules that is a “set of rules, applicable to electronic seal, which defines the requirements for their determination of whether an electronic seal is fit for a particular business or legal purpose”.

3. SCOPE

The electronic seal policy defined in the present document is suitable for a large range of business or application domains: B2B, B2C, G2B, G2C, G2G, C2C etc.
Examples of actual application are:

- G2C: Creation/sealing of e-permits or an attestation of residence.
- G2B: Creation/sealing of VAT-attestations, sealing of custom documents, etc.
- B2C: hospital sealing invoices or attestations for patients
- B2B: A company subscribing to an insurance contract.

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 to legal person used for electronic seal provided by Trust Service Providers. It is important that the following shall be followed:

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

- The legal person shall obtain suitable electronic sealing certificate from approved Trust Service Providers under the Saudi National PKI.

- By virtue of the data integrity featured by the Public Key Cryptography technology, no need to electronically sealing each and every page like in the paper world.

- Depends on the business requirements; the sealing may be an automated process without involvement of a human being; creator of the electronically sealing.

- For mass sealing (e.g. automated process), it shall be ensured that:
    - no data can be introduced in the flow of data to be sealed (network and application protection required);
    - the user is aware that more than one document is to be sealed and the data to be sealed are correctly “displayed”.

- The seal creation data can be stored on a secure server. It shall require the authentication of the authorised persons in order to allow the creation data to compute a seal.

- Depends on the business requirements; the electronic seal may be augmented. Augmenting seals is the process by which certain material (e.g. time stamps, validation data and even archival-related material) is incorporated to the seals for making them more resilient to change or for enlarging their longevity.

- An organisation shall use standard and recognised seal formats (e.g. XAdES, CAdES, PAdES etc.) if it decides to develop own seal creation application.

- 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 Trust Service Provider shall define identity verification requirements for legal 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 sealing certificates.

- Based on the assurance level electronic seal shall be either advanced or qualified offered to the legal person.

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

Certificate Level of Assurance	Electronic Seal legal level
High	Qualified
Medium	Advanced

- 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 organizational documents presented for establishing the legal person identity shall identify the legal person and confirm that the Authorizer is a member of the legal person.

- The Authorizer's association with the legal person (e.g. corporations, organization) shall be evidenced.

- Trust service providers issuing qualified certificates for electronic seals shall implement necessary measures in order to be able to establish the identity of the natural person representing the legal person to whom the qualified certificate for the electronic seal is provided.

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

- The issuer of the certificate to legal person 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 electronic seal issued to legal person shall comply with issuing CA CP and CPS.

- For subscribers using centralized Signing Platform, Signing keys used for sealing purpose 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 the legal person believes that the signer's private key was stolen or otherwise compromised, the legal person shall contact Trust Service Provider for revocation of certificate.

- 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 sealing application

9. REFERENCES

- [ENISA] Security guidelines on the appropriate use of qualified electronic seals, December 2016.