Cabinet Resolution No. (28) of 2023 Regarding the Executive Regulation of the Federal Decree-Law No. (46) of 2021 On Electronic Transactions and Trust Services

We, the UAE Cabinet,

- Having considered the Constitution; and
- Federal Law No. (1) of 1972 on the Competencies of Ministries and Powers of Ministers, as amended; and
- Federal Decree-Law no. (14) of 2021 Regarding the Establishment and Organization of the Federal Authority for Identity, Citizenship, Customs and Ports Security; and
- Federal Decree-Law No. (45) of 2021 Regarding the Protection of Personal Data; and
- Federal Decree-Law No. (46) of 2021 on Electronic Transactions and Trust Services; and
- Federal Decree-Law No. (42) of 2022 concerning Civil Procedures; and
- Acting upon the proposal of Director General of the Telecommunications and Digital Government Regulatory Authority (TDRA); and
- The approval of the Cabinet,

have issued the following Resolution:

Article (1)

Definitions

The definitions contained in the aforementioned Federal Decree-Law No. (46) of 2021 shall apply to this Resolution. The following words and expressions shall have the meanings assigned against each unless the context requires otherwise:

Decree-Law	:	Federal Decree-Law No. (46) of 2021, on Electronic Transactions and Trust Services.
Competent Authority	:	The Authority that issues the Trade License.
Termination Plan	:	A document that sets out the procedures related to the Licensee's plan and preparedness to terminate the services outlined in the License, pursuant to the Decree-Law and this Resolution and the decisions issued by the Authority (TDRA) in implementation of both of which, and the requirements of the Concerned Entities.
Service Practice Statement	:	A statement of practices used by the Trust Service Provider and the Qualified Trust Service Provider in the management and operation of services.

Service Policy	:	A specific set of rules setting out policies, procedures, technical data, roles and responsibilities related to the management and operation of Trust Services and Qualified Trust Services.
Subscriber	:	A Person that enters into a contract with the Trust Service Provider or with the Qualified Trust Service Provider to benefit from Trust Services or Qualified Trust Services provided by such provider.
Status of Qualified Service Provider	:	The status granted or withdrawn by the Authority (TDRA), as per the term of qualification and as listed in the UAE Trusted list, which confirms that the Qualified Trust Service Provider that provides such service is qualified for providing the same.
Encryption	:	A process intended to protect the confidentiality of data and information by converting data from a readable and understandable format into a non-understandable format in the form of codes, characters and figures.

Article (2)

License Application

1. The Authority shall publish the necessary information about all procedures, forms, and information that are required for licensing purposes on the Authority's website, or by any other means it deems appropriate.
2. The license application must include all the information requested by the Authority, and such information must be submitted in ways and means specified by the Authority.
3. The License Applicant undertakes to follow all procedures and use the application forms specified by the Authority.
4. The Authority shall specify the documents and data that must be included in the license application, provided that among such documents and data are the following:
   a. A copy of the license issued by the Competent Authority or the relevant governing body that grants the Applicant authorization to conduct said activities within the State.
   b. A statement indicating the business activities not relating to the Trust Services and Qualified Trust Services that the License Applicant is authorized to carry out.
   c. Details of the premises where the License Applicant conducts business in the State.
   d. A copy of the License Applicant's business plan, outlining the nature and strategy of its business, objectives, marketing plans, and service delivery plan.
   e. The type of trade License, the shares of partners therein, if any, and the organizational structure of the License Applicant.

f. A statement indicating the institutional and operational capacities of the License Applicant.
g. A Conformity Assessment Report of a term not exceeding a month.
h. A copy of the documents submitted during the Conformity Assessment Process set out in Clause (g) of this Article.
i. Services termination plan in accordance with the provisions of Article (18) of this Resolution.
j. A financial data report for the last fiscal year issued by a certified auditor in the State, proving the availability of financial resources equivalent to five million (5,000,000) Dirhams.
k. Submitting a bank guarantee or insurance determined by the Authority, which shall be automatically renewed upon the license renewal.
l. Evidence of payment of the license application fees by the means determined by the Authority.

Article (3)

Procedures for Examining License Application

1. The Authority shall complete the revision and examination of the license application and verify the information and documents submitted within one month from the date of completion of the application. In cases requiring additional time for review and verification, the License Applicant would be notified of the updated time period.
2. Should there be any modifications to the data or documents submitted in the license application that is justified, or if the License Applicant wishes to cancel the license application, the License Applicant must inform the Authority thereof within a week. The Applicant shall bear the fees and costs incurred therefrom.
3. The Authority may exempt the License Applicant from some of the licensing requirements set forth in this Resolution and the decisions issued by the Authority.

Article (4)

The Authority's Decision After Examining the License Application

1. The Authority shall issue its decision after reviewing and examining the License Application, as follows:
   a. Approving the License Application to provide certain Trust Services or Qualified Trust Services, if the Authority deems that the License Applicant has fulfilled the requirements stipulated in the Decree-Law, this Resolution, the decisions issued by the Authority in implementation thereof, and the requirements of the Concerned Entities.
   b. Rejecting the license application to provide certain Trust Services or Qualified Trust Services, if the Authority deems that the License Applicant has not met

the requirements stipulated in the Decree-Law, this Resolution, the decisions issued by the Authority in implementation thereof, and the requirements of the Concerned Entities.

2. If the Authority approves the License Application to provide Trust Services or Qualified Trust Services specified in the application:
   1) The Authority will issue a license authorizing the Applicant to provide the approved Trust Services or Qualified Trust Services after paying the license issuance fees.
   2) The Authority will update the UAE Trusted list in accordance with the licensing decision on the basis of each Trust Service or Qualified Trust Service specified in the license.
3. In case of approving the License Application to provide the Qualified Trust Services specified in the application, the Authority shall grant the License Applicant a license authorizing the Applicant to provide such services, grant the License Applicant the status of Qualified Service Provider and update the UAE Trusted list accordingly on the basis of each approved trust service specified in the license.

Article (5)

License Issuing Authority

The Authority shall issue the licensing decision after obtaining the approval of the Chairman or his delegate.

Article (6)

License Period

The license period is two years starting from the date of issuance of the license.

Article (7)

License Renewal Application

1. The Licensee undertakes to fulfill all requirements for the license renewal no less than three (3) months before the expiration of the license period, while taking into account the following:
   a. The license renewal application must include all the data and documents contained in Clause (4) of Article (2) of this Resolution, in addition to any other data or documents specified by the Authority.
   b. The license renewal application must include an evidence of payment of the fees for the license renewal application in the form and means determined by the Authority.

Article (8)

Failure to renew the license within the scheduled dates

A Licensee whose license period has expired without renewing the license thirty (30) days before its date of expiration is considered in violation, and administrative penalties shall be applied against the said Licensee in this regard.

Article (9)

Procedures for examining license renewal application

The Authority will review and verify the data and documents submitted for the license renewal application as per the procedures and requirements described in Article (3) of this Resolution.

Article (10)

License Renewal Decision

Upon review and verification of the license renewal application, the Authority shall issue its decision as follows:

1. Approval of the license renewal application, if the Authority deems that the renewal applicant has met the requirements stipulated in the Decree-Law, this Resolution, the decisions issued by the Authority in implementation thereof, and the requirements of the Concerned Entities. On this basis:
   a. The Authority will issue a license authorizing the Applicant to provide the approved Trust Services or Qualified Trust Services after paying the license issuance fees.
   b. The Authority will update the UAE Trusted list in accordance with the licensing decision on the basis of each Trust Service or Qualified Trust Service specified in the License Application.
2. Rejecting the license renewal application if the Authority deems that the License Applicant has not met the requirements stipulated in the Decree-Law, this Resolution, the decisions issued by the Authority in implementation thereof, and the requirements of the Concerned Entities, as the case may be. In this case, the Authority may take any of the following actions:
   a. Specify a time limit to address the non-conformity issues, after which the rejection decision will be reconsidered or ultimately approved.

b. Apply the administrative penalties in force in this regard.

Article (11)

Appealing Against the Authority's Decision

The License Applicant or Renewal Applicant whose application was rejected is entitled to resubmit a new application in accordance with the procedures in force in this regard, or to appeal within fourteen (14) days of the Authority's decision to reject such application.

Article (12)

Suspension or Cancellation of License

1. In the event that the license for the Trust Service Providers or the Qualified Trust Service Providers is suspended, the Licensee must immediately refrain from enrolling any new subscribers for the services specified in the license, while maintaining the continuity of service provision for the existing subscribers before the suspension decision takes effect.
2. In the event that the license for Trust Service Provider or the Qualified Trust Service Provider is canceled, a notification will be sent to them to start activating the Termination Plan for all or some of the services specified in the license, and to amend the UAE Trusted list upon completion of the Termination Plan.
3. In the event that the license of a Qualified Trust Services Provider is canceled, the Status of Qualified Service Provider shall be revoked for the services whose license is cancelled.
4. In all cases, the Licensee shall not, upon the expiration of the license period or its revocation, suspend the Trust Services or the Qualified Trust Services directly except in accordance with the procedures determined by the Authority. The Licensee shall not be exempted from the obligations specified in the Decree-Law, this Resolution, the decisions issued by the Authority in implementation thereof and the requirements of the Concerned Entities, as the case may be, except with the prior approval of the Authority.
5. Implementing the procedures contained in this Article does not prevent the application of administrative penalties or the fines stipulated in the Decree-Law.

Article (13)

Cases of Amending Licenses

1. The Licensee must notify the Authority within a week in the event of making any amendments or changes to the information submitted in the license or renewal application or in the documents submitted to obtain the Conformity Report.
2. The Licensee should obtain prior approval from the Authority in cases of amending or changing the data and information previously submitted to the Authority that are specified by the Authority, provided that the following data and information are included:
    a. Information about the establishment/enterprise, its ownership, and the location where the Licensee conducts business in the State.
    b. The technical, administrative and financial capacities to manage and operate the services specified in the license.
    c. Any changes in the procedures for the identity verification of the applicants and subscribers to the Trust Services or the Qualified Trust Services.
    d. Any changes to the information systems of the Trust Services or the Qualified Trust Services.
    e. Any modifications to the Termination Plan.
3. Changes that are made to the license, Trust Services, Qualified Trust Services, or the Status of Qualified Service Provider will be regularly included in the UAE Trusted list, should the change requires so, at the Authority discretion.
4. The Authority will determine the means for submitting requests of amendment and processing through decisions issued by the Authority

Article (14)

Bearing the costs of suspending or revoking the license

The Applicant for License Renewal or the Licensee whose Status of Qualified Service Provider is withdrawn or whose license is suspended or revoked, shall bear all expenses related to the Conformity Assessment Reports.

Article (15)

Licensee Obligations

The Licensee undertakes to do the following:

1. Submitting up-to-date and accurate data and documents to the Authority throughout the license period.
2. Acting in a fair and impartial manner in conducting all activities, operations, presentation and marketing of its services, in a way that does not cause monopoly or impact on the sector's competitiveness or the subscribers. This includes the Licensee's obligation to refrain from publishing incorrect or inaccurate information, or obstructing the mechanisms for implementing the Decree-Law, this Resolution,

decisions issued by the Authority in implementation thereof and the requirements of the Concerned Entities.

3. Bearing responsibility for damages that are intentionally or negligently caused to any person due to the Licensee's failure to fulfill the obligations under the provisions of the Decree Law, this Resolution, the decisions issued by the Authority in implementation thereof and the requirements of the Concerned Entities.
4. Informing the subscribers of the Trust Services or Qualified Trust Services provided by the Licensee of any restrictions on the use of these services before providing such services to subscribers, and not bearing any responsibility for the damages resulting from the use of such services in cases of exceeding those restrictions.
5. Adopting the appropriate policies that are based on assessments of the risks that would threaten the services provided by the Licensee, in addition to taking the adequate technical and regulatory measures that are necessary to manage legal, administrative, security, operational, and other direct and indirect risks, without prejudice to the levels of security and reliability, while being proportional to the level of the risk. In particular, due diligence and necessary measures must be taken in terms of:
    a. Procedures for registering and verifying subscribers and activating the services provided for them.
    b. Procedural and penal controls.
    c. Management and implementation of services.
    d. Preventing security incidents, minimizing their impact and informing the Concerned Entities, as the case may be, as well as the Subscribers and authorized authorities of the negative impacts of any of these incidents, if they occur.
    e. Safeguarding the cybersecurity protection of the Licensee's information systems in accordance with approved cybersecurity policies.
6. Taking all necessary technical and regulatory measures to comply with the Federal legislations related to the protection of data or personal data, thereby safeguarding and preserving the confidentiality of the subscriber's personal data. In addition, preventing access to, viewing or disclosing such data without obtaining the subscriber's consent and so far as is necessary to such service provision.
7. Notifying the Authority and subscribers immediately in the following cases:
    a. The Licensee's information systems are compromised with any risk that may affect the authenticity and integrity of the services provided.
    b. Subscribers' information or documents are compromised with unauthorized disclosure.
    c. The security of personal or non-personal information or data that are retained is breached, or they are lacking in terms of authenticity and integrity, thus affecting the services provided.
8. Prior to the provision of the Trust Services or the Qualified Trust Services, informing subscribers and Relying Parties, in a clear and accessible manner, of all terms and conditions related to the use of such services, including any restrictions on their use and the obligations and liabilities incurred by subscribers and Relying

Parties when using such services, and ensuring that the approval of the subscribers Relying Parties is obtained before starting to provide services to them.

9. Notifying the Party relying on the Trust Services or the Qualified Trust Services of the security and trust levels of the digital identity used as part of the services provision.
10. Ensuring compliance with the requirements, standards, controls and technical procedures for the security and trust levels specified in the Electronic Identification System approved by the Authority.
11. Developing a regularly updated Termination Plan to ensure continuity of service provision in accordance with the Decree-Law, this Resolution, the decisions issued by the Authority in implementation thereof and the requirements of the Concerned Entities. The Termination Plan must outline the following:
    a. Means of notifying subscribers when services are terminated or suspended.
    b. A mechanism to safeguard the integrity and reliability of the subscriber records.
    c. Methods of access to the subscriber records for the subscribers who are impacted by the service termination or suspension.
    d. Methods ensuring that the transactions and records carried out and created by the subscribers are not impacted during the course of the Trust Services provision by the Licensee.
12. Recording and retaining information that related to the data issued and received by the Licensee, especially for the purpose of providing evidence for any legal procedure or for the purpose of ensuring continuity of service provision, for a period of not less than fifteen (15) years from the date of establishing the key record, with the exception of evidence of identification that is used to issue the Authentication Certificate, which must be recorded and retained for a period of not less than ten (10) years from the date of expiration of such certificate, as well as allowing access to such information.
13. Establishing appropriate mechanisms to receive and address complaints in accordance with the requirements determined by the Authority.
14. Developing the Service Policy document and Service Practice Statement in accordance with the standards and controls issued by the Authority.
15. Meeting the standards and requirements issued by the Authority when determining the procedures for the service included in the Service Policy document and the Service Practice Statement.
16. Publishing the Service Policy and Service Practice Statement and their amendments to the public in Arabic and English, in a form that can be accessed electronically around-the-clock through the week.
17. Publishing the disclosure document for service provided, which briefly presents the main points of the service provision policy to the subscribers and Relying Parties.

Article (16)

Obligations of the Qualified Trust Service Provider (QTSP)

In addition to the obligations stipulated in Article (15) of this Resolution, the Qualified Trust Service Providers must adhere to the following controls and procedures:

1. Fair, honest and competent business conduct in the course of all their activities and operations.
2. Appointing individuals with specialized expertise in terms of the required and reliable practical and scientific competence and experience, who are appropriately accredited and trained in the rules of information security and personal data protection, and those who have knowledge of relevant national and international standards and specifications.
3. Securing sufficient financial resources to manage and operate the Qualified Trust Services
4. Using reliable and secure systems to store, process and protect data in a way that allows:
   a. Data retrieval, provided that prior consent is obtained from the data owner.
   b. Data entry, processing and modification only by authorized persons.
   c. Data validation.
5. Taking all necessary measures to combat the forgery, theft and illegal use of data.
6. Using technically reliable systems and products that guarantee technical security and are protected against any changes, modifications or breaches

Article (17)

Suspension of Services

1. The Licensee shall not suspend any of its activities or services without obtaining prior approval from the Authority.
2. Submitting a request to suspend the Trust Services or Qualified Trust Services shall be in accordance with the means determined by the Authority.
3. The Authority will respond to the request to suspend the Trust Services or the Qualified Trust Services within a period of one (1) month from the date of submitting the request. In cases that require more time for review and verification, the Licensee will be notified of the updated time period.
4. The Licensee must notify the Authority of its desire to suspend the provision of any, all, or part of the Trust Services or Qualified Trust Services for no less than three (3) months before the planned termination date.
5. The Licensee must inform the public, including the subscribers and Relying Parties, of its desire to suspend the provision of any, all, or part of its services for a period of no less than two (2) months before the planned termination date, and after obtaining the Authority's approval.
6. The Licensee must assist and enable the subscribers to move to another licensee that provides services similar to the services planned to be terminated, as the case may be, and in accordance with the controls and instructions established by the Authority.

7. The Licensee must take the necessary measures to ensure that the suspension of any of its service provision or part thereof does not disrupt the verification of the validity and reliability of their outputs, which would have been established before their actual termination.

Article (18)

Licensee's Obligations to activate the Termination Plan

The Licensee must activate its Termination Plan and take the following actions:

1. Revocation of all Authentication Certificates or the data of the subscriber's accounts issued by the Licensee for services to be terminated that have not been previously revoked or whose validity period will not expire before the Licensee terminates its services, whether the subscribers requested their revocation or not.
2. Revocation of all other relevant certificates.
3. Destroying, suspending, or preventing the use of all the Licensee's or subscribers' E-Signature or E-Seal Creation Data, including backup copies, so that the E-Signature or E-Seal Creation Data cannot be recovered.
4. The Licensee will continue to provide its services to the subscribers during the period of the Termination Plan approved by the Authority, and it shall not provide its services to any new subscriber from the activation date of the Termination Plan.

Article (19)

Advanced E-Signatures (AdES) and Advanced E-Seals (AdESeal)

1. The Advanced E-Signature (AdES) and Advanced E-Seal (AdESeal) must meet the encryption's specifications and standards, the mechanism and requirements for creating the E-Signature or E-Seal, the information security controls and the additional requirements specified under the decisions issued by the Authority.
2. The Advanced E-Signature (AdES) and Advanced E-Seal (AdESeal) must be created in accordance with one or more of the forms and formats defined in accordance with the decisions issued by the Authority.

Article (20)

Qualified E-Signatures (QES) and Qualified E-Seals

The Qualified E-Signature (QES) and Qualified E-Seal must meet the following requirements:

1. Meeting the conditions under the decisions issued by the Authority as stipulated in Article (19) of this Resolution at the time of signing.

2. Preserving the integrity of signed Data.
3. The E-Signature Creation Device Qualified E-Seal Creation Device meeting the requirements contained in Article (26) of this Resolution.
4. Any additional requirements determined by the Authority in accordance with the decisions issued by the Authority in implementation of the Decree-Law, this Resolution and the requirements of the Concerned Entities.

Article (21)

Approved Authentication Certificate Requirements for E-Signatures and E-Seals

1. The approved Authentication Certificate for E-Signatures and E-Seals must include the following:
   a. A wording or indication, in a form at least suitable for automated processing, stating that the certificate has been issued as an approved Authentication Certificate for E-Signatures or E-Seals.
   b. A set of data that unequivocally identifies the Qualified Trust Service Provider who issues the Authentication Certificates for the E-Signatures and E-Seals, including references to the United Arab Emirates as the State in which the provider provides such service. Such data must include: The name and ID Number of the Qualified Trust Service Provider as shown in the official records.
   c. A set of data that unequivocally represents the identity of the holder of the E-Signature or E-Seal, provided that this data includes:
      1) The full name of the Signatory and, if applicable, the ID Number as stated in the official records
      2) A Pseudonym, and if used, it must be clearly stated.
   d. E-Signature or E-Seal verification data that corresponds to the E-Signature or E-Seal Creation Data.
   e. Details of the beginning and end period of validity of the approved Authentication Certificate for E-Signature or E-Seal.
   f. The Identification Code of the approved Authentication Certificate for the E-Signature or E-Seal, which must be unique to the Qualified Trust Service Provider.
   g. The Qualified E-Signature (QES) and Qualified E-Seal issued by the Qualified Trust Service Provider issuing the approved Authentication Certificate for the E-Signature or E-Seal.
   h. Free link to download the approved Authentication Certificate for the E-Signature or E-Seal.
   i. The services website that can be used to inquire about the validity of the approved Authentication Certificate for the E-Signature or E-Seal.
2. If there is E-Signature or E-Seal Creation Data related to the verification process of the E-Signature authenticity in a Qualified E-Signature Creation Device, this must be indicated in the approved Authentication Certificate for the E-Signature or E-Seal in an appropriate form that can be processed automatically.

3. The approved Authenticity Certificate for the E-Signature or E-Seal may include certain additional, non-mandatory features that do not affect the interoperability and recognition of the Qualified E-Signature or Qualified E-Seal.
4. The Authority may add any other requirements in the approved Authentication Certificate for the E-Signature or E-Seal in accordance with the decisions issued by the Authority in implementation of the Decree-Law, this Resolution and the requirements of the Concerned Entities.

Article (22)

Revoking Authentication Certificates

If the approved Authentication Certificate for the E-Signature or E-Seal is revoked after its issuance, it would lose its validity upon its immediate revocation, and in no case may the certificate be reactivated.

Article (23)

Prohibiting Temporary Suspension of Authentication Certificates

The Licensee is prohibited from temporarily suspending the approved Authentication Certificates for the E-Signature or E-Seal, or temporarily suspending them for the period of their validity after their activation.

Article (24)

Issuing the approved Authentication Certificate for E-Signature or E-Seal

1. Authentication Certificates for E-Signatures or E-Seals shall exclusively be issued as a Qualified Trust Service by a Qualified Trust Service Provider.
2. The Qualified Trust Service Providers may use an approved Authentication Certificate for E-Signature or E-Seal that is issued by another Qualified Trust Service Provider and supported by a Qualified and valid E-Signature or E-Seal, to authenticate a Person requesting an approved Authentication Certificate for E-Signature or E-Seal.
3. In the event that the Qualified Trust Service Provider uses a procedure equivalent to personal attendance to verify the identity and capacity of the Person to whom an approved Authentication Certificate for E-Signature or E-Seal will be issued, in accordance with Clause (4) of Article (34) of the Decree-Law, the Authority, in addition to the Conformity Assessment Report, may ensure that such procedure is

equivalent to reliability of personal attendance, in accordance with the controls and regulations issued by the Authority in this regard.

4. A Qualified Trust Service Provider, who issues an approved Authentication Certificate for an E-Signature or E-Seal as a Qualified Trust Service, must create and update a database of certificates.
5. A Qualified Trust Service Provider must specify the appropriate set of policies and practices for providing an approved Authentication Certificate for an E-Signature or E-Seal as a Qualified Trust Service under the Service Policy for providing approved Authentication Certificates for E-Signature or E-Seal as a Qualified Trust Service, in addition to the Service Practice Statement for such service.
6. The Service Policy and Service Practice Statement shall be subject to the terms and technical specifications for the content and structure of the policies defined in accordance with the decisions issued by the Authority.
7. The Qualified Trust Service Provider shall be liable for providing the Qualified Trust Service in accordance with the procedures stipulated in the Service Practice Statement and Service Policy. If the Trust Service or part of it is provided by external third-parties, the Qualified Trust Service Provider must determine the responsibilities of those parties and ensure their commitment to implementing any controls required by the Qualified Trust Service Provider.

Article (25)

Revoking the Authentication Certificate for E-Signature or E-Seal

1. If the Qualified Trust Service Provider who issued an approved Authentication Certificate for an E-Signature or E-Seal decided to revoke the certificate upon its owner's request or for reasons specified by the Service Provider, he must record the revocation in its Certificate database and publish the Certificate Revocation Status on the Certificate Validation Service within a period not exceeding Twenty-four (24) hours from the date of request receipt from the certificate holder, and the revocation shall come into effect upon its publication.
2. The Qualified Trust Service Provider must provide any Relying Party with any information related to the validity or revocation of Authentication Certificates issued by the Provider, even after the expiration of the approved Authentication Certificate for the E-Signature or E-Seal and for a period of at least fifteen (15) years from its expiration, provided that this information is free of charge and can be accessed automatically at all times.

Article (26)

Issuance of the Qualified E-Signature Device and Qualified E-Seal Device

1. The issuance of a Qualified E-Signature Device or a Qualified E-Seal Device for Signatories as a Qualified Trust Service shall only be conducted by a Qualified Trust Service Provider compliant with the technical, security, procedural, and regulatory specifications and standards set forth in an Authority-issued decision.
2. The Qualified Trust Service Provider must determine a set of appropriate policies and practices to provide the Qualified E-Signature and Qualified E-Seal Creation Devices as a Qualified Trust Service. In all cases, these policies and practices must meet the technical conditions and specifications for the content and structure, which are determined in a decision issued by the Authority.
3. The Qualified E-Signature or the Qualified E-Seal Creation Device must meet the requirements of Article (21) of the Decree-Law. The Qualified E-Signature or the Qualified E-Seal Creation Device must be certified by the Certification Bodies for such devices, whether public or private, provided that these Certification Bodies are accredited by the Authority.
4. The Qualified Trust Service Provider must adhere to the standards and requirements for security assessment of information technology technologies, products and services issued by the Authority to approve the Qualified E-Signature or Qualified E-Seal Creation Devices.
5. Certification Bodies for the Qualified E-Signature or the Qualified E-Seal Creation Devices must adhere to the list of standards and requirements issued by the Authority. Any certification granted to any of those bodies or any of the devices certified by them will be revoked if it is proven that they violate such standards and requirements.
6. The handling, generation, or duplication of E-Signature Creation Data on behalf of the Signatory is forbidden unless conducted by a Qualified Trust Service Provider offering a Qualified Trust Service specifically for overseeing the remote management of a Qualified E-Signature Device.
7. The Qualified Trust Service Provider must only use the Qualified E-Signature Creation Devices and Qualified E-Seal Creation Devices that are approved by the Authority.
8. The Authority will develop, publish and manage a list of Certification Bodies for the Qualified E-Signature Creation Devices, Qualified E-Seal Creation Devices and other devices that have been certified by them, in addition to a dated record showing the status of these bodies and the status of approvals for certifying such devices.
9. The Qualified Trust Service Provider must follow the conditions and procedures issued by the Authority to apply for approval to use the Qualified E-Signature Creation Devices and Qualified E-Seal Creation Devices, in order to be included in the list referred to in Clause (8) of this Article.
10. If the Certification for E-Signature Creation Devices or Qualified E-Seal Creation Devices is revoked by the issuing Certification Bodies, the Applicant commits to notifying the Authority within two (2) weeks of the revocation date. In such instances, the Authority is empowered to initiate measures or request the Qualified Trust Service Provider to assess the impact on the Licensed Services and subsequently take necessary actions based on the assessment findings.

Article (27)

Remote Management of the Qualified E-Signature Device and the Qualified E-Seal Device

1. The Qualified E-Signature Creation Devices and the Qualified E-Seal Creation Devices will be managed remotely, as a Qualified Trust Service, by the Qualified Trust Service Provider, who must adhere to the following:
   a. Creating and managing the Qualified E-Signature Creation Data and the Qualified E-Seal Creation Data on behalf of the Signatory.
   b. Copying E-Signature Creation Data for backup purposes only, provided that the following are met:
      1) The security level of the copied data sets must be the same as the original data sets.
      2) The number of copied data sets should not exceed the minimum required to ensure the service continuity.
   c. Ensuring compliance with any requirements specified in the Certification Certificate for the Qualified E-Signature and the Qualified E-Seal Remote Creation Device, issued pursuant to Article (26) of this Resolution.
2. The Authority will issue decisions related to technical standards and specifications related to Clause (1) of this Article.
3. The Qualified Trust Service Provider must determine the appropriate set of policies and practices to provide the remote management service for the Qualified E-Signature and the Qualified E-Seal Remote Creation Devices as a Qualified Trust Service. In all cases, those policies and practices must meet the technical conditions and specifications for the content and structure, which are determined in a decision issued by the Authority.
4. The Qualified Trust Service Provider shall be responsible for providing the Qualified Trust Service in accordance with the procedures stipulated in the Service Practice Statement and Service Policy. If the Trust Service, or part of it, is provided by external third-parties, the Qualified Trust Service Provider must determine the responsibilities of those parties and ensure their commitment to implementing any Controls required by the Qualified Trust Service Provider.

Article (28)

Preservation of Qualified E-Signature/E-Seal Data

1. The Qualified Trust Service Provider shall exclusively provide the Qualified E-Signature or Qualified E-Seal Data Preservation Service on the condition that the Provider applies procedures and technologies that extend the trust validity period of the Qualified E-Signature or the Qualified E-Seal beyond the technical validity period, as determined in a decision issued by the Authority. Such procedures and

technologies shall not affect the reliability of the Qualified E-Signature and the Qualified E-Seal.

2. The Qualified Trust Service Provider undertakes to maintain the trust validity of the Qualified E-Signature and the Qualified E-Seal for a period of not less than fifteen (15) years from the date of the preservation request.
3. The Qualified Trust Service Provider shall retain all information necessary to verify the authenticity of the Qualified E-Signature or Qualified E-Seal until the end of the preservation period.
4. The Qualified Trust Service Provider must ensure the integrity, quality and clarity of the Qualified E-Signature and Qualified E-Seal data preserved by the Provider, and allow the data to be used properly either by subscribers or by another Qualified Trust Service Provider who provides a Qualified Trust Service, subject to the express consent of the subscribers.
5. The preservation proof issued by the Qualified Trust Service Provider must be signed or sealed using a reliable E-Signature or a reliable E-Seal issued by the Provider.
6. The Qualified Trust Service Provider must determine the appropriate set of policies and practices to provide the Qualified E-Signature and the Qualified E-Seal Data Preservation Service as a Qualified Trust Service. In all cases, these policies and practices must meet the technical conditions and specifications for the content and structure, as determined in a decision issued by the Authority.
7. The Qualified Trust Service Provider commits to providing the Qualified Service in accordance with the procedures stipulated in the Service Practice Statement and Service Policy. If the Trust Service, or a part thereof, is provided by external third-parties, the Qualified Trust Service Provider must determine the responsibility of those parties and ensure their commitment to implementing any required controls by the Qualified Service Provider.

Article (29)

Archiving Digital Documents

The Government Entities are required to adhere to the following guidelines when archiving electronic documents containing an Advanced or Qualified E-Signature or an Advanced or Qualified E-Seal:

1. Maintaining the integrity of the E-Signature or E-Seal from any change.
2. Maintaining the E-Signature or E-Seal from any deletion.
3. Ensuring that the E-Signature or E-Seal is re-created on the new document in the event of any permitted change to the electronic document.

Article (30)

Authenticity Verification of the Qualified E-Signature or Qualified E-Seal

1. The Qualified Trust Service Provider shall exclusively provide the Qualified E-Signature or Qualified E-Seal Authenticity Verification Service, on the condition that the Provider is compliant with the provisions of Article (20) of the Decree-Law and the service is in accordance with the decisions issued by the Authority in this regard.
2. The Service Provider for the Qualified E-Signature and Qualified E-Seal authenticity verification is required to determine the appropriate policies and practices for validating the authenticity of Qualified E-Signatures and Qualified E-Seals.
3. Time information added to the authenticity verification result of a Qualified E-Signature or Qualified E-Seal must be generated using a Qualified Time Stamp.
4. The Qualified Trust Service Provider commits to providing the Qualified Trust Service in accordance with the procedures stipulated in the Service Practice Statement and Service Policy. If the Qualified Trust Service or part thereof is provided by external third-parties, the Qualified Trust Service Provider must determine the responsibility of those parties and ensure their commitment to implementing any controls. required by the Qualified Trust Service Provider.
5. The Authority will issue the decisions related to technical standards and specifications that must be adhered to by the Qualified Service Provider, including:
   a. The operational and security controls, service management mechanism, physical security requirements, requirements for technical and security examination testing processes for the service before its provision to the subscribers, and technical and security examination reports.
   b. The requirements related to listing the Qualified E-Signature/Qualified E-Seal Authenticity Verification Service as a Qualified Trust Service in the UAE Trusted list.

Article (31)

Qualified Electronic Time Stamp Creation Service

1. The Qualified Trust Service Provider shall exclusively provide the Qualified Electronic Time Stamp Creation Service, on the condition that the Provider is compliant with the provisions of Article (23) of the Decree-Law and the Service is in accordance with the decisions issued by the Authority in this regard.
2. The Qualified Trust Service Provider that provides the Qualified Electronic Time Stamp Creation service must determine the appropriate set of policies and practices for creating the Qualified Electronic Time Stamp. In all cases, those policies and practices should meet the technical conditions and specifications for the content and structure, which are determined in a decision issued by the Authority.
3. The Qualified Trust Service Provider who provides the Qualified Electronic Time Stamp Creation service commits to providing this service in accordance with the procedures stipulated in the Service Practice Statement and the Service Policy. If the Trust Service or part of it is provided by external third-parties, the Qualified Trust Service Provider must determine the responsibility those parties and ensure

their commitment to implementing any controls required by the Qualified Service Provider.

4. The Authority will issue the decisions related to technical standards and specifications that must be adhered to by the Qualified Service Provider, including:
   a. The Service Policy and Service Practice Statement mentioned in Article (15) of this Resolution.
   b. The requirements related to listing the service on the UAE Trusted list.

Article (32)

Qualified Electronic Delivery Service

1. The Qualified Electronic Delivery Service may only be provided by a Qualified Trust Service Provider that meets the provisions of Article (24) of the Decree-Law and in accordance with the decisions issued by the Authority in this regard.
2. The Qualified Electronic Delivery Service Provider must determine the identity of the Sender and Consignee based on a high level of security and trust and with a high degree of trust and acceptance, which eliminates any risks and prevents misuse or manipulation of the identity of the Sender and Consignee.
3. The Qualified Electronic Delivery Service Provider must determine the appropriate set of policies and practices for providing the Qualified Electronic Delivery Service. In all cases, those policies and practices must meet the technical conditions and specifications for the content and structure, which are determined in a decision issued by the Authority.
4. The Qualified Electronic Delivery Service Provider shall be responsible for providing the service in accordance with the procedures stipulated in the Service Practice Statement and Service Policy. In the event that the Trust Service or part of it is provided by external third-parties, the Qualified Electronic Delivery Service Provider must determine the responsibility of those parties and ensure their commitment to implementing any controls required by the Qualified Service Provider.
5. The Authority will issue decisions related to the technical standards and specifications that must be adhered to by the Qualified Electronic Delivery Service Provider, including:
   a. The Service Policy and Service Practice Statement stipulated in Article (15) of this Resolution.
   b. The requirements for the Electronic Delivery Service messaging and the manuals used.
   c. The requirements related to listing the service on the UAE Trusted list.
6. Data sent and received using the Qualified Electronic Delivery Service shall be considered evidence of the integrity of the data sent, sent by an identified Sender and received by an identified Consignee, in addition to the accuracy of the date of sending and receipt indicated by the Qualified Electronic Delivery Service.

Article (33)

Conformity Assessment

1. It is not permissible for an entity that does not obtain the approval and certification of the Authority to conduct a Conformity Assessment for the purposes of implementing the Decree-Law, this Resolution, the decisions issued by the Authority in implementation thereof and the requirements of the Concerned Entities.
2. The Conformity Assessment Body (CAB) must be accredited and registered with the Authority.
3. The Conformity Assessment Body must develop a report stating the extent to which the License Applicant or Licensee and the services, which they will work to provide or is providing, conform and meet the requirements contained in the Decree-Law, this Resolution, the decisions issued by the Authority in implementation thereof and the requirements of the Concerned Entities.
4. The Conformity Assessment reports will be issued in accordance with the specifications and procedures determined by the Authority.
5. The Conformity Assessment Body must avoid any conflict of interest, whether actual or potential, to conduct the Conformity Assessment of the License Applicant or Licensee, and the Authority shall determine the necessary standards and controls in this regard.
6. The Authority will issue the decisions related to the technical standards and specifications that must be adhered to by Conformity Assessment Bodies (CABs), including:
   a. The mechanisms for accrediting the Conformity Assessment Bodies.
   b. The rules of scrutiny to be adhered to by the Conformity Assessment Bodies (CABs) while assessing the conformity of the Trust Service Providers or Qualified Trust Service Providers and the services they provide.

Article (34)

UAE Trusted list

1. The Authority shall develop a list entitled the "UAE Trusted list" in accordance with its specifications, and publish it on its website. This list will include the following:
   a. Information about the Trust Service Providers and the Trust Services they provide and a statement of their license status.
   b. Information about the Qualified Trust Service Providers and the Qualified Trust Services they provide and a statement of the license status and Status of Qualified Service Provider.
2. The information indicated in Clause (1) of this Article shall be provided by the Trust Service Providers or Qualified Trust Service Providers in a definite and documented

manner through their conformity reports issued by the Conformity Assessment Body or the Authority.

3. The Authority will issue the decisions related to the standards, technical specifications and procedures for the UAE Trusted list, such as the form and content, the mechanism for publishing the List, maintaining and amending it, and the mechanism for reading and using it by the Relying Parties.
4. The Authority must include the Licensee in the UAE Trusted list on the basis of the services specified in the license.
5. Upon including the Licensee on the UAE Trusted list, the Authority must link each service specified in the license to a digital identifier that allows the service to be uniquely and clearly identified, in accordance with the technical specifications and decisions issued by the Authority in this regard.

Article (35)

Qualified Trust Mark

1. The Authority shall determine, publish and manage standards relating to the form, content and presentation of the Qualified Trust Mark for the Qualified Trust Services.
2. A Qualified Trust Service Provider may use the granted Qualified Trust Mark as follows, provided that the Status of Qualified Service Provider is referred to in the UAE Trusted list of the Qualified Trust Service Providers:
   a. Receive the Status of Qualified Service Provider and licenses necessary for the Qualified Service Provider in accordance with the Decree-Law, this Resolution, the decisions issued by the Authority in implementation thereof and the requirements of the Concerned Entities.
   b. Indicate in a clear and non-misleading manner the Qualified Trust Services, the granted Status of Qualified Service Provider, and the effective license obtained by the Qualified Trust Services Provider.
   c. Provide a hyperlink to the Qualified Trust Mark that indicates the Status of Qualified Service Provider, the status of the effective license, and the Qualified Trust Services contained on the UAE Trusted list, in accordance with the requirements and resolutions issued by the Authority.

Article (36)

Repeals/Abrogation

Every provision that contradicts or conflicts with the provisions of this Resolution shall be abrogated

Article (37)

Publication and Entry into Effect of the Resolution

This Resolution shall be published in the Official Gazette and shall come into effect after ninety (90) days from the date of its publication.

Mohammed bin Rashid Al Maktoum

Prime Minister of the United Arab Emirates

On: 09/Ramadan/1444H
Corresponding to: 31/March/2023