قرار رقم (51) لسنة 2023م
بشأن
اعتماد الضوابط والمعايير الفنية المطبقة على مزودي خدمات الثقة وخدماتهم

رئيس مجلس إدارة الهيئة العامة لتنظيم قطاع الاتصالات والحكومة الرقمية،،،،

بعد الاطلاع على المرسوم بقانون اتحادي رقم (3) لسنة 2003 في شأن تنظيم قطاع الاتصالات ولائحته التنفيذية وتعديلاتهما،

وعلى المرسوم بقانون اتحادي رقم (46) لسنة 2021 بشأن المعاملات الإلكترونية وخدمات الثقة ولائحته التنفيذية،

وبناءً على ما عرضه مدير عام الهيئة العامة لتنظيم قطاع الاتصالات والحكومة الرقمية، وموافقة مجلس إدارة الهيئة في اجتماعه المنعقد بتاريخ 18 ديسمبر 2023م، وعلى مذكرة الموافقة المرفوعة إليه من إدارة الهيئة،

قررنا ما يلي:

المادة (١)

يُعتمد بموجب هذا القرار "الضوابط والمعايير الفنية المطبقة على مزودي خدمات الثقة وخدماتهم" المُرفقة بهذا القرار.

المادة (٢)

يُعمل بهذا القرار اعتباراً من تاريخ صدوره، ويُنشر في الجريدة الرسمية.

صدر بتاريخ 18 ديسمبر 2023م.

ص.ب. 26662 • أبوظبي، الإمارات العربية المتحدة ABU DHABI, UNITED ARAB EMIRATES • فاكس 7772229 2 971+ FAX • الرقم المجاني 800 12 TOLL FREE
www.tdra.gov.ae

The technical controls and standards applicable to trust service providers and the trust services they provide

Issue Date: 18 Dec. 2023

Telecommunications and Digital Government Regulatory Authority (TDRA)
P O Box 26662, Abu Dhabi, United Arab Emirates (UAE)
www.tdra.gov.ae

References

Reference	Title
[Law (46) 2021]	Federal Decree Law No. (46) of 2021 On Electronic Transactions and Trust Services
[Reg (28) 2023]	Federal Executive Regulation No. (28) of 2023
[UAE TL Specifications]	Resolution on the technical specifications and formats relating to the United Arab Emirates trusted list pursuant to Article 34 of the Executive Regulation No. (28) of 2023
[TL onboarding guide for third parties]	Guidelines for relying parties on the interpretation of the UAE trusted list
[SOG-IS Crypto WG]	SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms (https://www.sogis.eu/uk/supporting_doc_en.html)
[X.509]	ISO/IEC 9594-8:2020/Recommendation ITU-T X.509: Information technology - Open Systems Interconnection - The Directory - Part 8: Public-key and attribute certificate frameworks.
[RFC 3647]	IETF RFC 3647: Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework
[RFC 3161]	IETF RFC 3161: Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)
[ETSI TS 119 102-2]	ETSI TS 119 102-2 V1.4.1 (2023-06): Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report
[ETSI EN 319 122-1]	ETSI EN 319 122-1 V1.3.1 (2023-06): Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: "Building blocks and CAdES baseline signatures".
[ETSI EN 319 132-1]	ETSI EN 319 132-1 V1.2.1 (2022-02): Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures
[ETSI EN 319 142-1]	ETSI EN 319 142-1 V1.1.1 (2016-04): Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures
[ETSI EN 319 162-1]	ETSI EN 319 162-1 V1.1.1 (2016-04): Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: "Building blocks and ASiC baseline containers".
[ETSI TS 119 182-1]	ETSI TS 119 182-1 V1.1.1 (2021-03): Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures
[ETSI EN 319 401]	ETSI EN 319 401 v2.3.1 (2021-05): Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[ETSI EN 319 403]	ETSI EN 319 403 V2.3.1 (2020-06): Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.
[ETSI EN 319 403-1]	ETSI EN 319 403-1 V2.3.1 (2020-06): Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers.
[ETSI TS 119 403-3]	ETSI TS 119 403-3 V1.1.1 (2019-03): Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers.
[ETSI EN 319 411-1]	ETSI EN 319 411-1 v1.4.1 (2023-10): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

[ETSI EN 319 411-2]	ETSI EN 319 411-2 v2.5.1 (2023-10): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
[ETSI EN 319 412-1]	ETSI EN 319 412-1 v1.5.1 (2023-09): Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
[ETSI EN 319 412-2]	ETSI EN 319 412-2 v2.3.1 (2023-09): Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
[ETSI EN 319 412-3]	ETSI EN 319 412-3 v1.3.1 (2023-09) : Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
[ETSI EN 319 412-5]	ETSI EN 319 412-5 v2.4.1 (2023-09): Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
[ETSI EN 319 421]	ETSI EN 319 421 V1.2.1 (2023-05): Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
[ETSI EN 319 422]	ETSI EN 319 422 V1.1.1 (2016-03): Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
[ETSI TS 119 431-1]	ETSI TS 119 431-1 V1.2.1 (2021-05): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev
[ETSI TS 119 431-2]	ETSI TS 119 431-2 V1.2.1 (2023-06): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation
[ETSI TS 119 432]	ETSI TS 119 432 V1.2.1 (2020-10): Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation
[ETSI TS 119 441]	ETSI TS 119 441 V1.2.1 (2023-10): Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services
[ETSI TS 119 442]	ETSI TS 119 442 V1.1.1 (2019-02): Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services
[ETSI TS 119 511]	ETSI TS 119 511 v1.1.1 (2019-06): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques
[ETSI TS 119 512]	ETSI TS 119 512 v1.2.1 (2023-05): Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services
[ETSI TS 119 612]	ETSI TS 119 612 v2.2.1 (2016-04): Electronic Signatures and Infrastructures (ESI); Trusted Lists
[CEN EN 419 231]	CEN EN 419 231: Protection profile for trustworthy systems supporting time stamping.
[CEN TS 419 261]	CEN TS 419 261: Security requirements for trustworthy systems managing certificates and time stamps
[CABF Network]	CA/Browser Forum: Network and certificate system security requirements
[CABF Guidelines]	CA/Browser Forum: Guidelines for The Issuance and Management of Extended Validation Certificates
[CABF Baseline]	CA/Browser Forum: Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates
[RFC 5280]	IETF RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[ISO 15408]	ISO/IEC 15408:2022 (parts 1 to 3): Information security, cybersecurity and privacy protection - Evaluation criteria for IT security
[ISO 18045]	ISO/IEC 18045:2022: Information security, cybersecurity and privacy protection— Methodology for IT security evaluation
[ISO 17065]	ISO/IEC 17065:2012, Conformity assessment - Requirements for bodies certifying products, processes and services.

[ISO 17067]	ISO/IEC 17067:2013, Conformity assessment - Fundamentals of product certification and guidelines for product certification schemes.
[ISO 27001]	ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection- Information security management systems Requirements
[FIPS PUB 140-2]	FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules"
[ISO 14641]	ISO 14641:2018: Electronic document management — Design and operation of an information system for the preservation of electronic documents — Specifications

Abbreviations

CAB	Conformity Assessment Body
CAR	Conformity Assessment Report
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider
DCP	Domain Validation Certificate Policy
EIAC	Emirates International Accreditation Centre
EU	European Union
EUMS	European Union Member State
EVCP	Extended Validation Certificate Policy
IVCP	Individual Validation Certificate Policy
LCP	Lightweight Certificate Policy
NAB	National Accreditation Body
NCP	Normalized Certificate Policy
NCP+	Extended Normalized Certificate Policy
OCSP	Online Certificate Status Protocol
OVCP	Organizational Validation Certificate Policy
OVR	General requirement (requirement applicable to more than 1 component)
PDS	PKI Disclosure Statement
QC	Qualified Certificate
QcStatement	Qualified Certificate Statement
QESig	Qualified Electronic Signature
QESeal	Qualified Electronic Seal
QSCD	Qualified electronic Signature/Seal Creation Device in the sense of [Law (46) 2021].
QTS	Qualified Trust Service
QTSDS	QTS Disclosure Statement(s)
QTSP	Qualified Trust Service Provider
remoteQSCDaaS	Remote Qualified electronic Signature/Seal Creation Device as a Service

SCDev	Signature Creation Device
SVR	Signature Validation Report
TSAPS	Time-Stamping Authority Practice Statement
TSP/TS	Trust Service Provider and the Trust Service(s) it provides
TSU	Time-Stamping Unit
TL	Trusted List
TLS	Transport Layer Security
TDRA	Telecommunications And Digital Government Regulatory Authority
TS	Trust Service
TSP	Trust Service Provider
UAE	United Arab Emirates
UAE-QSCD	QSCD in the sense of [Law (46) 2021]
VSP	Validation Service Policy
VSPS	Validation Service Practice Statement

Definitions

The terms, words, and phrases used in this Resolution shall have the same meaning as are ascribed to them in the Federal Decree Law No. (46) of 2021 On Electronic Transactions and Trust Services unless this Resolution expressly provides for otherwise, or the context in which those terms, words and phrases are used in this Resolution requires otherwise. For the purposes of this Resolution, the following terms and words shall have the meanings ascribed to them below:

"The Authority"	the Telecommunications and Digital Government Regulatory Authority ("the TDRA");
"**UAE qualified electronic signature**"	qualified electronic signature as specified in [Law (46) 2021];
"**UAE qualified electronic seal**"	qualified electronic seal as specified in [Law (46) 2021];
"**UAE qualified signature creation device**"	qualified signature creation device as defined in [Law (46) 2021]
UAE qualified seal creation device"	qualified seal creation device as defined in [Law (46) 2021]
"TDRA-approved CAB"	conformity assessment body competent for carrying out conformity assessment of a qualified digital trust service provider and the qualified digital trust services it provides as specified in [Reg (28) 2023];

1 Introduction

The Authority is competent to issue controls, procedures and standards related to trust services and qualified trust services.

Accordingly, the present document specifies security and policy requirements on the operation and management by qualified and non-qualified trust service providers of the qualified and non-qualified trust services they provide.

The requirements laid down in the present document are applicable to all qualified and non-qualified trust service providers, but in particular:

(a) Pursuant to Article 15(14) and Article 15(15) of the [Reg (28) 2023], the licensee shall comply with the technical specifications and requirements set out in section 2.

(b) Pursuant to Article 19(1) of the [Reg (28) 2023], the provision of a service for the creation of advanced electronic signatures and advanced electronic seals shall comply with the technical specifications and requirements set out in section 5 and section 13.2.

(c) Pursuant to Article 19(2) of the [Reg (28) 2023], advanced electronic signatures and advanced electronic seals shall comply with the technical specifications and requirements set out in section 13.

(d) Pursuant to Article 21(4) of the [Reg (28) 2023], qualified certificates for electronic signature and qualified certificates for electronic seal shall comply with the technical specifications and requirements set out in section 6.4 and section 6.5 respectively.

(e) Pursuant to Article 24(6) of the [Reg (28) 2023], qualified trust service providers providing qualified certificates for electronic certificate and qualified trust service providers providing qualified certificates for electronic seal shall comply with the certificate policy requirements set out in section 6.

(f) Pursuant to Article 26(1) and Article 26(2) of the [Reg (28) 2023], qualified trust service providers providing of qualified signature creation devices to signatories and qualified trust service providers providing of qualified seal creation devices as a qualified trust service shall comply with the technical specifications and requirement set out in section 11.

(g) Pursuant to Article 27(2) and Article 27(3) of the [Reg (28) 2023], qualified trust service providers providing management services of remote qualified signature creation devices and qualified trust service providers providing management services of remote qualified seal creation devices as a qualified trust service shall comply with the policies and practice statements requirements and technical specifications set out in section 10.

(h) Pursuant to Article 28(1) and Article 28(6) of the [Reg (28) 2023], qualified trust service providers providing qualified preservation of qualified electronic signatures and qualified trust service providers providing qualified preservation of qualified electronic seals as a qualified trust service shall comply with the

policies and practice statements requirements and technical specifications set out in section 8.

(i) Pursuant to Article 30(1) and Article 30(5) of the [Reg (28) 2023], qualified trust service providers providing validation of qualified electronic signatures and qualified trust service providers providing validation of qualified electronic seal as a qualified trust service shall comply with the technical specifications and requirements set out in section 9.

(j) Pursuant to Article 31(1) and 31(4) of the [Reg (28) 2023], qualified trust service providers providing qualified timestamping services shall comply with the technical specifications and requirements set out in section 7.1.

(k) Pursuant to Article 32(1) and Article 32(5) of the [Reg (28) 2023], qualified trust service providers providing qualified electronic delivery services shall comply with the technical specifications and requirements set out in section 12.1.

2 General provisions for all trust services provided by a trust service provider

2.1 General requirements

GPR-1	The TSP shall implement an information security management system covering the scope of the trust service, for which it shall obtain an ISO/IEC 27001 certification or an equivalent certification approved by TDRA.
GPR-2	The TSP shall implement the recommendations of the CA/Browser Forum network security guide [CABF Network], items 1 to 4, where every occurrence of “CA system” shall be read as “TSP system” and where in item 4.c "CA/Browser Forum" is replaced by "TDRA".
GPR-3	The TSP shall conform to [ETSI EN 319 401] with the amendments provided in the subsequent clauses of the present section, which shall prevail over the corresponding requirements of [ETSI EN 319 401].
GPR-4	The risk assessment and mitigation plan specified in [ETSI EN 319 401]-clause 5 shall be regularly reviewed and revised: at least on a yearly basis; and - at any change having an impact on the TS provided, in particular when changing the provisions of the applicable trust service policy (e.g. CP) and/or trust service practice statement (e.g. CPS) and in case of changes identified in section 2.4 “Notifications”.
GPR-5	The liability insurance referred to in [ETSI EN 319 401] REQ-7.1.1-04 shall be of at least AED five [5] Millions per year.
GPR-6	The maximum interval between two checks for changes in the configuration of the TSPs systems which violate the TSPs security policies, shall be [one week].
GPR-7	Regarding REQ-7.7-01 of [ETSI EN 319 401], requirements for the trustworthy systems managing certificates and time-stamps shall be ensured by using systems conforming to [CEN TS 419 261] or to a suitable protection profile (or profiles), defined in accordance with ISO/IEC 15408 [ISO 15408].

2.2 Facility, Management, Operational and Security Controls

The following requirements regarding the facility, the management, the operational and security controls shall be respected:

OPS-1	Any update to the risk assessment and mitigation plan shall be notified to TDRA together with the notification of changes referred to in section 2.4 “Notifications” below.

OPS-2	The TSP shall use all legal means it may need to verify the honesty of the personnel it uses for the provisioning of its TS, including outsourcers or subcontractors. In particular, the TSP shall verify that it has not been established by a final judgement or a final administrative decision that a member of the personnel is guilty for an offense in contradiction with the tasks (s)he has been allocated by the TSP. This includes being guilty of critical professional misconduct: - by having violated applicable laws or regulations or ethical standards of the profession to which the person belongs, or - by having engaged in any wrongful conduct which has an impact on its professional credibility where such conduct denotes wrongful intent or gross negligence. This includes fraud, significant deficiencies in performance of a contract, distortion of competition, corruption, participation in a criminal organization, money laundering or terrorist financing, terrorist-related offences or offences linked to terrorist activities, child labour or other forms of trafficking in human beings.
OPS-3	The verifications in **OPS-2** shall be performed prior to the allocation of a trusted role and reviewed regularly, at least every two (2) years.

2.3 Cryptography and cryptographic suites

The TSP is subject to requirements concerning the cryptography and cryptographic suites:

CRY-1	The cryptographic suites and the cryptographic key lengths and parameters used by the TSP shall be capable to resist to cryptographic attacks during the validity period of the data to which they are applied and, when applicable, of the associated certificate, whichever is the longer.
CRY-2	The cryptographic suites and the cryptographic key lengths and parameters shall conform to the latest version of the SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms [SOG-IS Crypto WG].

2.4 Notifications

NTF-1	To the exception of editorial changes, the TSP shall notify to TDRA the changes it intends to make in its policies and practice statement(s) [60] sixty days prior implementation. Once approved by TDRA, the TSP shall notify its subscribers and relying parties of the changes it intends to make in its policies and practice statement [30] thirty days prior implementation.
NTF-2	Intended changes that must be notified to TDRA include but are not limited to:

	- Changes of practices resulting from a change in trust service policy or associated terms and conditions of use; - Changes of outsourcers or subcontractors; - Changes of hosting conditions; - Changes of cryptographic material; - Modifications in the technical architecture; - Changes in the procedures for identifying, authenticating and registering subscribers/subjects; - Changes in the governance of the TSP; - Changes resulting in a modification of the UAE trusted list with regards to the TSP and the TS it provides; - Termination of trust services or part thereof.
NTF-3	On a yearly basis, the TSP shall notify TDRA with an overview of all changes made to the provision of its TS having an impact on the statements made in the conformity assessment report.

2.5 Termination

TER-1	The termination plan referred to in REQ-7.12-02 of [ETSI EN 319 401] shall comply with the requirements of section 2.6 “Structure and content of the termination plan of a trust service provided by a trust service provider” in terms of format and content, particularly to cover the scheduled and unscheduled termination, partial or global termination.

TER-2	The documentation associated to a TS termination plan shall include the following:
	- Formal termination procedures;
	- Formal termination procedures internal assessment, including regular internal assessment of the practical feasibility of the implementation of the termination plan;
	- Formal termination procedures training;
	- Formal termination procedures internal assessment reports;
	- Formal termination procedures auditing reports;
	- Formal termination (contractual) arrangements with third parties (incl. subcontractors, taking over parties, the TDRA, etc.);
	- QTS terms and conditions, practices and policy documents;
	- Up-to-date documentations for personal data protection rules compliancy:
	  o Treatment registers and data (and metadata) mapping;
	  o Privacy impact assessments;
	  o Documents (e.g. binding corporate rules) for particular cases of transfer outside the UAE;
	- As part of the risk management obligations from [Law (46) 2021]:
	  o A termination-specific risk analysis shall be undertaken, documented and the associated mitigation measures shall be documented and their implementation regularly controlled.
	  o This analysis shall include a personal data impact assessment and documentation of the associated mitigation measures.

TER-3	As part of the necessary measures the TSP shall undertake to ensure that the termination of the TS does not cause disruption in validating the trustworthiness of the outcomes of a TS that would have been created before its effective termination: 1) The TSP shall ensure the recording, the preservation and the availability of all information that are related to the data issued and received by it for an appropriate duration (i.e. at least fifteen years from original record creation, save identification evidence for a period of ten years from the date of expiry of qualified and non-qualified certificates), including after the TS has been effectively terminated; 2) The data referred to in the obligation of the previous point shall include: a) where TSP are providing qualified certificates as a QTS, the certificate database of all certificates issued by the TSP, including subscriber certificates, when the QTS to be terminated consisted in the issuance of qualified certificates, and b) the identification evidence collected as a part of the provision of the TS or the QTS to be terminated.

2.6 Structure and content of the termination plan of a trust service provided by a trust service provider

2.6.1 Front page

1. Document name & identification
   This clause shall include versioning, date of entering into force, status and document classification.
2. (Q)TSP identification
   This clause shall clearly identify the name of the (Q)TSP, and where applicable its registration number, as stated in the official records, its official postal address and its contact electronic address.
3. Identification of concerned (Q)TS
   This clause shall identify the (Q)TS covered by the termination plan.

2.6.2 Introduction

1. Overview
   This clause shall provide a general overview of the termination plan and a synopsis of the (Q)TSP/(Q)TS to which termination provisions apply.
   A diagrammatic representation shall be provided.
   All participants and (Q)TS service components shall be identified.
2. Document name and identification rules
   This clause shall provide any applicable names or other identifiers for the termination plan document and for relevant referenced documents, when applicable.
3. (Q)TS to which the termination plan applies
   This clause shall provide a detailed identification of the (Q)TS to which termination provisions apply, in particular with regards to the UAE trusted list service entry(ies) and the associated “Service digital identity” elements (i.e. public keys when based on PKI).
   A diagram, or table representation, shall be provided.

4. Termination plan administration
   This clause shall provide the name and mailing address of the organization or authority that is responsible for the drafting, registering, maintaining, and updating of the termination plan.
   It shall identify the responsibilities and duties of that organization or authority with regards to the (Q)TSP/(Q)TS termination, termination plan reviewing, internal / external auditing processes, and its execution.
   This clause shall include the name, electronic mail address, telephone number, and fax number of a contact person, service or functional role.
5. Applicable national legislation and relevant provisions on (Q)TSP/(Q)TS termination
   This clause shall provide references to the applicable UAE legislation and identify the relevant UAE legal provisions on (Q)TSP/(Q)TS termination.
6. Definitions and abbreviations
   This clause shall contain a list of definitions for defined terms used within the document, as well as a list of abbreviations used in the document and their meanings.

2.6.3 Termination plan provisions

The termination plan provisions shall include the following fields:

2.6.3.1 Scheduled termination

This clause shall describe the provisions and actions to be undertaken:

- In the context of the scheduled termination of part or of whole of the (Q)TS to which the termination plan applies; and/or
- In the context of the scheduled actions that could result in the partial or complete termination of the (Q)TS to which the termination plan applies.

The arranged/contracted custodian(s), insurers or 3rd parties involved in assisting the implementation of the termination shall be properly identified and their role and scope of assistance shall be clearly described.
The relevant actions and the associated provisions shall include, at least:

- Termination plan update and the provisions on its notification to the TDRA;
- Identification of the operations to be ceased and the expected timing/scheduling;
- Identification of the expected impact on the relevant entries of the UAE trusted list;
- Risk analysis update and updated mitigation measures;
- Identification of the financial resources and/or appropriate insurance to cover the costs required to properly execute the termination plan;
- Personal data impact assessment update and updated mitigation measures;
- Termination notifications and related actions:
  - Identification of the entities to be notified of the termination (e.g. the TDRA, subscribers, relying parties, other (Q)TSP with which the terminated service has trust relationships, (Q)TSP staff and/or subcontractors);
  - For each notified entity or logical group of notified entities, specify the provisions on the termination notifications, the notification means and the expected timing/scheduling of those notifications;
  - Identification of the associated documentation;
  - Identification of the services whose termination is scheduled, the reason for such termination and the expected timing/scheduling;

- Terms and conditions ruling the notified termination: This may include:
  - Arrangement(s) applicable with another (Q)TSP for the provision of future (Q)TS of similar nature;
  - Preservation of subscriber's related (personal) data;
  - Preservation of operational data and other relevant data to sustain the trustworthiness of the (Q)TS outputs and related evidences;
  - With regards to qualified certificates, the conditions on their revocation (for unexpired and unrevoked certificates);
  - Foreseen compensations to subscribers, when applicable;

- Procedures for the execution of the termination actions;
- Identification of the personnel (staff and/or subcontractors), their requested expertise and the training conditions;
- Transfer of recorded, auditing and archival records to the arranged/contracted custodian(s), and proper identification of custodian(s);
- Description of the procedures and mechanisms put in place to ensure the integrity and trustworthiness of all the data preserved after the termination;
- Identification of the methods enabling the users impacted by the termination of the TS to access their preserved records;
- Description of the procedures and mechanisms put in place to ensure that transactions and records created before the termination are not impacted by the termination.

2.6.3.2 Unscheduled termination

This clause shall describe the provisions and actions to be undertaken:

- In the context of the unscheduled termination of part or of whole of the (Q)TS to which the termination plan applies; and/or
- In the context of the unscheduled actions that could result in the partial or complete termination of the (Q)TS to which the termination plan applies.

Unexpected or unscheduled termination of the (Q)TSP/(Q)TS may result from different causes such as severe incident or disaster from which incomplete or unsatisfactory recovery could be reached, bankruptcy, court orders, and any unexpected reason forcing the (Q)TSP/(Q)TS to execute a termination.
This clause shall address provisions and actions like those covered in clause 2.6.3.1 "Scheduled termination" above, considering the unexpected and unscheduled nature of the causes for termination and the potential significant decrease of delays within which those actions need to be undertaken.
The arranged / contracted custodian(s), insurers or 3rd parties involved in assisting the implementation of the unscheduled termination should be properly identified and their role and scope of assistance should be clearly described.

2.6.4 Internal/external compliance audit and other assessments

This clause shall address internal and external audit and other assessment, in particular:

- The list of topics covered by the assessment and/or the assessment methodology used to perform the assessment.
- Frequency of compliance audit or other assessment.
- The identity and/or qualifications of the personnel performing the audit or other assessment.
- The relationship between the assessor and the (Q)TSP whose termination plan is being audited/assessed, including the degree of independence of the assessor.
- Actions taken as a result of deficiencies found during the termination plan audit or other assessment.

- Internal/external person(s) entitled to be communicated the results of an assessment, and/or the actions taken as a consequence.

2.6.5 Other provisions

This clause provides any other applicable provisions not fitting in any above clause.

3 Specific provisions for trust service providers issuing certificates for electronic signatures and/or certificates for electronic seals

3.1 General requirements

GPR-1	The TSP issuing certificates for electronic signatures and/or certificates for electronic seals (hereafter the TSP) shall conform to [ETSI EN 319 411-1] with the amendments provided in the subsequent articles of the present document, which have precedence on specifications from [ETSI EN 319 411-1].
GPR-2	References made in [ETSI EN 319 411-1] to [ETSI EN 319 401] shall be understood as referring to the version of that standard amended according to section 2 “General provisions for all trust services provided by a trust service provider” of the present document.
GPR-3	References made in [ETSI EN 319 411-1] to [ETSI EN 319 412-2] shall be understood as referring to the version of that standard amended according to section 3.5 “Content profile for certificates for electronic signatures” of the present document.
GPR-4	References made in [ETSI EN 319 411-1] to [ETSI EN 319 412-3] shall be understood as referring to the version of that standard amended according to section 3.6 “Content profile for certificates for electronic seals” of the present document.

3.2 Certificate policies and certification practice statement

CPS-1	The TSP shall specify and maintain the set of policies and practices appropriate for the issuance of certificates it provides as a trust service under the form of certificate policies (CP) and certification practice statement (CPS) in conformance with clauses 5 and 7 of [ETSI EN 319 411-1] provided: a. The TSP's CP and CPS shall be structured in accordance with IETF [RFC 3647]. b. (i) The TSP's CP and CPS shall be identified by means of unique object identifiers of the form required in Recommendation ITU-T [X.509]. (ii) The corresponding TSP's own CP identifier shall be included in the issued certificate. c. The TSP shall publicly disclose its CPS, its CP(s) and their revisions through an online means that is available on a 24x7 basis. d. The TSP shall publish PKI Disclosure Statement(s) (PDS) that summarize key points of its certificate policy(ies) for the benefit of subscribers and relying parties. e. The PKI Disclosure Statement(s) (PDS) shall be structured in accordance with Annex A of [ETSI EN 319 411-1].

	f. The TSP shall publish an English translation of its CPS, CP(s) and PDS(s). g. The TSP's CP shall specify the requirements for the use of certificate profiles.
CPS-2	The certificates issued under the [NCP], [NCP+] or [LCP] requirements are aimed to support the advanced electronic signatures based on a (non-qualified) certificate for electronic signatures or for electronic seals as defined in [Law (46) 2021].
CPS-3	The [EVCP], [OVCP], [IVCP], and [DVCP] certificate policies and all associated requirements defined in [ETSI EN 319 411-1] are out of scope and not applicable.
CPS-4	In clause 5.4.2 of [ETSI EN 319 411-1], the concept of operation of devices reflected by the terms "operated" & "operating" is replaced by the concept of having final responsibility and liability for the device, for the activation of the electronic signature or electronic seal creation data and for the creation of the electronic signature or electronic seal. The terms "operated" & "operating" are replaced accordingly.
CPS-5	The TSP shall retain overall responsibility for the provision of the TS it provides and for conformance with the procedures prescribed in its CPS and its CPs or the CPs it supports, even when the TSP's functionality, or part of it, is undertaken by outsourcers. To this extent, the TSP shall define the outsourcers' liability and ensure that outsourcers are bound to implement any controls required by the TSP.

3.3 Facility, Management, Operational and Security Controls

OPS-1	The recommendation in [ETSI EN 319 411-1]-OVR-6.4.4-02 is turned into an obligation (i.e. the term "should" is replaced by "shall").

3.4 Issuance, management and revocation of non-qualified certificates

CCY-1	The TSP shall proceed to the registration, the management and the revocation of certificates in conformance with [ETSI EN 319 411-1], in particular with its clauses 6.1, 6.2, and 6.3, with the following amendments: Once a certificate is activated or accepted which ever event comes first, the TSP shall not proceed to the suspension of the certificate.
CCY-2	With regards to end-entity certificate rekey, the same rules apply as for the initial request.
CCY-3	With regards to end-entity certificate renewal, the TSP shall issue a new certificate using the subject's previously certified public key, only if its cryptographic security is still sufficient for the new certificate's validity period and no indications exist that the subject's private key has been compromised nor that the certificate has been revoked due to any other security breach.

CCY-4	With regards to end-entity certificate modification, the same rules apply as for the initial request.
CCY-5	The TSP shall be able to provide information regarding the validity or revocation of certificates issued by them at least fifteen (15) years after their expiry.

3.5 Content profile for certificates for electronic signatures

PSI-1	Certificates for electronic signatures shall contain: a. an indication, at least in a form suitable for automated processing, that the certificate has been issued as a certificate for electronic signature; b. a set of data unambiguously representing the trust service provider issuing the certificates including at least - the identification of the UAE where the TSP must be established and: - for a legal person: the full name and, where applicable, registration number as stated in the official records, - for a natural person: the person's name; c. at least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated; d. electronic signature validation data that corresponds to the electronic signature creation data; e. details of the beginning and end of the certificate's period of validity; f. the certificate identity code, which must be unique for the trust service provider; g. the advanced electronic signature or advanced electronic seal of the issuing trust service provider; h. the location where the certificate supporting the electronic signature or electronic seal referred to in point (g) is available free of charge; i. the location of the services that can be used to enquire about the validity status of the certificate.
PSI-2	Certificates for electronic signatures shall conform to [ETSI EN 319 412-2] to the exception of clause 5 and with the following amendments: a. GEN-4.4.1-3 of clause 4.4.1 of [ETSI EN 319 412-2] must read "*The Authority Information Access extension shall include an accessMethod OID, id-ad-caIssuers, with an accessLocation value specifying at least one access location of a valid CA certificate of the issuing CA. At least one access location shall use the http (http://) IETF RFC 7230-7235 [3] scheme or https (https://) IETF RFC 2818 [5] scheme.*" b. Certificates that have been issued as certificates for electronic signature shall contain the QcType 1 QcStatement described in clause 4.2.3 of [ETSI EN 319 412-5]. c. The organizationIdentifier attribute shall be included in the identity of the issuer, when the issuer is a legal person (amending clause

	4.2.3.1 of [ETSI EN 319 412-2]) in compliance with clause 5.1.4 of [ETSI EN 319 412-1] d. When a natural person subject is associated with an organization, the subject attributes shall also identify such organization using the attributes: e. organizationName including the full name of the organization as stated in the official records, and f. organizationIdentifier (amending clause 4.2.4 of [ETSI EN 319 412-2]) including in compliance with clause 5.1.4 of [ETSI EN 319 412-1] the registration number as stated in the official records. g. The Key Usage Type A as specified in clause 4.3.2 of [ETSI EN 319 412-2] Shall be used exclusively h. GEN-4.3.3-2 of [ETSI EN 319 412-2] is amended so that it reads: "*The certificate policies extension shall be present and shall contain the identifier of at least one certificate policy which reflects the practices and procedures undertaken by the CA and that is established and managed by the CA.*" i. When applicable, certificates for electronic signatures may include a declaration of a limitation on the value of transaction for which a certificate can be used. When this is the case, such declaration shall be implemented by means of the declarative statement specified in clause 4.3.2 of [ETSI EN 319 412-5]. j. When applicable, certificates for electronic signatures may include a declaration of a retention period for material information relevant to the use of and reliance on a certificate, expressed as a number of years after the expiry date of the certificate. When this is the case, such declaration shall be implemented by means of the declarative statement specified in clause 4.3.3 of [ETSI EN 319 412-5]. k. Certificates for electronic signatures shall include URLs to the applicable PKI Disclosure Statements (PDS) in accordance with Annex A of [ETSI EN 319 411-1]. This shall be implemented in conformance with clause 4.3.4 of [ETSI EN 319 412-5]. l. The end of the validity period (expiry date) of a certificate for electronic signature shall not exceed the end of the validity period (expiry date) of the issuing CA.

3.6 Content profile for certificates for electronic seals

PSE-0	All certificate fields and extensions shall comply with [ETSI EN 319 412-3] with the amendments specified in the present document. All references to [ETSI EN 319 412-2] made in [ETSI EN 319 412-3] shall be understood as referring to the version amended according to section 3.5 "Content profile for certificates for electronic signatures" of the present document.
PSE-1	Certificates for electronic seals shall contain: a. an indication, at least in a suitable from for automated processing, that the certificate has been issued as a certificate for electronic seal;

	b. a set of data unambiguously representing the trust service provider issuing the certificates including at least : - the identification of the UAE where the TSP must be established and: - for a legal person: the full name and, where applicable, registration number as stated in the official records, - for a natural person: the person's name; c. at least the name of the creator of the seal and, where applicable, registration number as stated in the official records; d. electronic seal validation data that corresponds to the electronic seal creation data; e. details of the beginning and end of the certificate's period of validity; f. the certificate identity code, which must be unique for the trust service provider; g. the advanced electronic signature or advanced electronic seal of the issuing trust service provider; h. the location where the certificate supporting the electronic signature or electronic seal referred to in point (g) is available free of charge; i. the location of the services that can be used to enquire about the validity status of the certificate.
PSE-2	Certificates for electronic seals shall conform to [ETSI EN 319 412-3] to the exception of clause 5 and with the following amendments: a. GEN-4.4.1-3 of clause 4.4.1 of [ETSI EN 319 412-2] must read "*The Authority Information Access extension shall include an accessMethod OID, id-ad-caIssuers, with an accessLocation value specifying at least one access location of a valid CA certificate of the issuing CA. At least one access location shall use the http (http://) IETF RFC 7230-7235 [3] scheme or https (https://) IETF RFC 2818 [5] scheme.*" b. Certificates that have been issued as certificates for electronic seal shall contain the QcType 2 QcStatement described in clause 4.2.3 of ETSI EN 319 412-5 [ETSI EN 319 412-5]. c. The organizationIdentifier attribute shall be included in the identity of the issuer, when the issuer is a legal person (amending clause 4.2.3.1 of [ETSI EN 319 412-2]) in compliance with clause 5.1.4 of [ETSI EN 319 412-1] d. The organizationIdentifier attribute shall be included in the identity of the subject to include, in compliance with clause 5.1.4 of [ETSI EN 319 412-1], the organization's registration number as stated in the official records. e. The organizationName attribute included in the identity of the subject shall include the full name of the organization as stated in the official records. f. The Key Usage Type C or D as specified in clause 4.3.2 of [ETSI EN 319 412-2] shall be used to the exclusion of any other combination. g. When applicable, certificates for electronic seals may include a declaration of a limitation on the value of transaction for which a certificate can be used. When this is the case, such

	declaration shall be implemented by means of the declarative statement specified in clause 4.3.2 of [ETSI EN 319 412-5]. h. When applicable, certificates for electronic seals may include a declaration of a retention period for material information relevant to the use of and reliance on a certificate. The retention period should be expressed as a number of years after the expiry date of the certificate. When this is the case, such declaration shall be implemented by means of the declarative statement specified in clause 4.3.3 of [ETSI EN 319 412-5]. i. Certificates for electronic seals shall include URLs to the applicable PKI Disclosure Statements (PDS) in accordance with Annex A of [ETSI EN 319 411-1]. This shall be implemented in conformance with clause 4.3.4 of [ETSI EN 319 412-5]. j. The end of the validity period (expiry date) of a certificate for electronic seal shall not exceed the end of the validity period (expiry date) of the issuing CA.

3.7 Provisions related to the inclusion of the related trust service in the UAE trusted list

TL-1	A TS consisting in the issuance of non-qualified certificates for electronic signatures or for electronic seals is identified in the UAE trusted list by means of a digital certificate of root-CA, an intermediate CA or an issuing CA.
TL-2	The confirmation by an accredited CAB and the verification by TDRA of the conformity of the TSP and the TS it provides with the requirements of [Law (46) 2021] and of the applicable TDRA resolutions must allow the demonstration that under the CA identified in TL-1 above, it is possible to distinguish without any ambiguity qualified certificates from non-qualified certificates, and certificates for electronic signatures from certificates for electronic seals.
TL-3	The TSP shall not include in non-qualified certificates any data or attribute that might lead to identify them erroneously as qualified.

4 Specific provisions for trust service providers issuing (non-qualified) certificate for website authentication

4.1 General requirements

GPR-0	TSP issuing certificates for website authentication shall comply with [Law (46) 2021] and with the General provisions for TSP/TS from section 2 “General provisions for all trust services provided by a trust service provider” of the present document.
GPR-1	The TSP, established in the UAE, issuing certificates for website authentication (hereafter the TSP): - shall conform to the "Guidelines for The Issuance and Management of Extended Validation Certificate" [CABF Guidelines] and "Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates" [CABF Baseline], appropriate to the type of certificate they provide, with the amendments provided in the subsequent articles of the present document, which have precedence on specifications from [CABF Guidelines] and [CABF Baseline]; - shall conform to [ETSI EN 319 401].
GPR-2	The foreign (non-UAE) CSP issuing certificates for website authentication (hereafter the CSP): - shall conform to the "Guidelines for The Issuance and Management of Extended Validation Certificate" [CABF Guidelines] and "Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates" [CABF Baseline], appropriate to the type of certificate they provide, with the amendments provided in the subsequent articles of the present document, which have precedence on specifications from [CABF Guidelines] and [CABF Baseline]; - shall be recognized by Google, Apple, Microsoft, Mozilla, Oracle (Java) & Adobe.

4.2 Certificate policies and certification practice statement

CPS-1	The TSP shall specify and maintain the set of policies and practices appropriate for the issuance of certificates it provides as a trust service under the form of certificate policies (CP) and certification practice statement (CPS) in conformance with clauses 6.1 of [ETSI EN 319 401] provided: a. The TSP's CP and CPS: (i) shall be structured in accordance with IETF [RFC 3647]; (ii) shall include the complete CA hierarchy, including root and subordinate CA's;

	(iii) shall include the signature algorithms and parameters employed; (iv) shall specify the practice regarding the use of CA keys for signing certificates, CRLs and OCSP; (v) shall include a clear statement that where a TSP includes a hierarchy of subordinate CAs up to a root CA, the TSP shall be responsible for ensuring the subordinate-CAs comply with the applicable policy requirements b. (i) The TSP's CP and CPS shall be identified by means of unique object identifiers of the form required in Recommendation ITU-T [X.509]. (ii) The corresponding TSP's own CP identifier shall be included in the issued certificate. c. The TSP shall publicly disclose its CPS, its CP(s) and their revisions through an online means that is available on a 24x7 basis. d. The TSP shall publish PKI Disclosure Statement(s) (PDS) that summarise key points of its certificate policy(ies) for the benefit of subscribers and relying parties. e. The TSP shall publish an English translation of its CPS, CP(s) and PDS(s). f. The TSP's CP shall specify the requirements for the use of certificate profiles.
CPS-2	The TSP shall retain overall responsibility for the provision of the TS it provides and for conformance with the procedures prescribed in its CPS and its CPs or the CPs it supports, even when the TSP's functionality, or part of it, is undertaken by outsourcers. To this extent, the TSP shall define the outsourcers' liability and ensure that outsourcers are bound to implement any controls required by the TSP.

4.3 Facility, Management, Operational and Security Controls

OPS-1	The TSP implements a security management system for which it shall obtain an ISO/IEC 27001 certification or equivalent.
OPS-2	The TSP shall establish and maintain an incident management and notification plan.
OPS-3	The TSP shall establish and maintain a business continuity (or disaster recovery) plan.
OPS-4	The TSP shall establish and maintain a termination plan in conformance with the requirements of section 2.5
OPS-5	Requirements for the trustworthy systems shall be ensured by using systems conforming to [CEN TS 419 261] or to a suitable protection profile (or profiles), defined in accordance with ISO/IEC 15408 [ISO 15408].

4.4 Issuance, management and revocation of non-qualified certificates

CCY-1	The TSP shall proceed to the registration, the management and the revocation of certificates in conformance with [CABF Guidelines] and [CABF Baseline], whichever reference is appropriate with regards to the type of certificate issued, provided: a. Once a certificate is activated or accepted which ever event comes first, the TSP shall not proceed to the suspension of the certificate. b. With regards to end-entity certificate rekey, the same rules apply as for the initial request. c. With regards to end-entity certificate renewal, the TSP shall issue a new certificate using the subject's previously certified public key, only if its cryptographic security is still sufficient for the new certificate's validity period and no indications exist that the subject's private key has been compromised nor that the certificate has been revoked due to any other security breach. d. With regards to end-entity certificate modification, the same rules apply as for the initial request.
CCY-2	The TSP shall be able to provide information regarding the validity or revocation of certificates issued by them at least fifteen (15) years after their expiry.
CCY-3	The TSP shall not include in non-qualified certificates any data or attribute that might lead to identify them erroneously as qualified.
CCY-4	The CSP shall not include in non-qualified certificates any data or attribute that might lead to identify them erroneously as qualified in the sense of the laws of the UAE.

4.5 Provisions related to the inclusion of the related trust service in the UAE trusted list

TL-1	The CSP shall not be included in the UAE trusted list.
TL-2	A TS provided by a TSP consisting in the issuance of non-qualified certificates for electronic signatures or for electronic seals is identified in the UAE trusted list by means of a digital certificate of a root-CA, of an intermediate CA or of an issuing CA.
TL-3	The confirmation by an accredited CAB and the verification by TDRA of the conformity of the TSP and the TS it provides with the requirements of [Law (46) 2021] and of the applicable TDRA resolutions must allow the demonstration that under the CA identified in TL-1 above, it is possible to distinguish without any ambiguity qualified certificates from non-qualified certificates, and certificates for electronic signatures from certificates for electronic seals.

5 Specific provisions for trust service providers creating electronic signatures and electronic seals as a trust service

5.1 General requirements

GPR-1	The TSP providing trust service (TS) consisting in the creation of electronic signatures and/or electronic seals (hereafter referred to as the TSP) shall conform to [ETSI TS 119 431-2] for the TS it provides with the amendments provided in the subsequent articles, which have precedence on specifications from [ETSI TS 119 431-1].
GPR-2	References made in [ETSI EN 319 431-2] to [ETSI EN 319 401] shall be understood as referring to the version of that standard amended according to section 2 “General provisions for all trust services provided by a trust service provider” of the present document.
GPR-3	When the TSP is managing the signing and/or sealing private keys on behalf of the signatories and/or creator of the seals, it shall conform to [ETSI TS 119 431-1].
GPR-4	The TSP **should** conform to [ETSI TS 119 432].
GPR-5	References made in [ETSI TS 119 431-2] to [ETSI TS 119 431-1] shall be understood as referring to the fixed version of that standard as indicated in [ETSI TS 119 431-1].
GPR-6	References made in [ETSI TS 119 431-2] to "(EU) advanced electronic signatures" and "(EU) advanced electronic seal" are replaced respectively by references to advanced electronic signatures and to advanced electronic seals as defined in [Law (46) 2021].
GPR-7	References made in [ETSI TS 119 431-2] to "(EU) qualified electronic signatures" and "(EU) qualified electronic seal" are replaced respectively by references to qualified electronic signatures and to qualified electronic seals as defined in [Law (46) 2021].
GPR-8	References made in [ETSI TS 119 431-2] to “eIDAS Regulation (EU) No 910/2014" are replaced by references to [Law (46) 2021].
GPR-9	Requirements stated in [ETSI TS 119 431-2] as applicable to "EU qualified certificates" shall apply mutatis mutandis to qualified certificates issued under [Law (46) 2021].
GPR-10	References made in [ETSI TS 119 431-2] to "EUMS trusted list" shall be understood as references to UAE trusted list.

5.2 Trust service policy and trust service practice statement

TPS-1	The TSP shall specify and maintain the set of policies and practices, as well as the documentation, appropriate for the TS it provides under the form of TS service policies and TS practice statement (TSPS) in conformance with [ETSI TS 119 431-2], and with [ETSI TS 119 431-1] when applicable, provided:

	a. The TSP's TS policies and TSPS shall be structured in accordance with [ETSI TS 119 431-2], and with[ETSI TS 119 431-1] when applicable. b. The TSP's TS policies and TSPS shall be identified by means of unique object identifiers of the form required in Recommendation ITU-T [X.509]. c. The TSP shall publicly disclose its TS policies, its TSPS, and their revisions through an online means that is available on a 24x7 basis. d. The TSP shall publish TS Disclosure Statement (TSDS) that summarizes key points of its TS policy(ies) for the benefit of subscribers and relying parties. e. The TSP shall publish an English translation of its TSPS, TS policies and TSDS(s).
TPS-2	The TSP shall retain overall responsibility for the provision of the TS it provides and for conformance with the procedures prescribed in its practices and its own validation service policies or the validation service policies it supports, even when the TSP's functionality, or part of it, is undertaken by outsourcers. To this extent, the TSP shall define the outsourcers' liability and ensure that outsourcers are bound to implement any controls required by the TSP.
TPS-3	The TSP shall create electronic signatures and/or electronic seals in accordance with one or more of the following standardized formats: - CAdES format: [ETSI EN 319 122-1], from the CAdES-B-T level; - XAdES format: [ETSI EN 319 132-1], from the XAdES-B-T level; - PAdES format: [ETSI EN 319 142-1], from the PAdES-B-T level; - JAdES format: [ETSI TS 119 182-1], from the JAdES-B-T level; - Signature container format - ASiC: [ETSI EN 319 162-1], from the corresponding B-T level.
TPS-4	Time-stamps added by the QTSP when creating electronic signatures and/or electronic seals shall be qualified electronic time stamps conformant with [Law (46) 2021].

5.3 Facility, Management, Operational and Security Controls

OPS-1	The trustworthy systems used by the TSP and the TS it provides **should** be certified against [ETSI TS 119 431-2], and against [ETSI TS 119 431-1] when applicable.

5.4 Provisions related to the inclusion of the related trust service in the UAE trusted list

TL-1	The TSP shall have for each instance of the creation of electronic signatures and/or electronic seals as a TS it provides, one (non-PKI based) service digital identifier as defined in clause 5.5.3 of [ETSI TS 119 612] which allows to uniquely and unambiguously identify the service within the UAE trusted list as specified hereafter.

TL-2	A TS consisting in the creation of electronic signatures and/or electronic seals is identified in the UAE trusted list by means of: a. In case no PKI public key technology is used to identify the TS, an indicator expressed by a URI which uniquely and unambiguously identifies the type of TS.

6 Specific provisions for qualified trust service providers issuing qualified certificates

6.1 Certificate policies

The present section defines four (4) certificate policies:

1. A policy for UAE qualified certificates issued to natural persons (UAE-QCP-n) offering the level of quality defined in [Law (46) 2021] for UAE qualified certificates. The identifier for this policy is: 2.16.784.1.1.8.1.1
2. A policy for UAE qualified certificates issued to legal persons (UAE-QCP-l) offering the level of quality defined in [Law (46) 2021] for UAE qualified certificates. The identifier for this policy is: 2.16.784.1.1.8.1.2
3. A policy (UAE-QCP-n-qscd) for UAE qualified certificates issued to natural persons offering the level of quality defined in [Law (46) 2021] for UAE qualified certificates and requiring the use of a UAE Qualified Signature Creation Device (QSCD). The identifier for this policy is: 2.16.784.1.1.8.1.3
4. A policy (UAE-QCP-l-qscd) for UAE qualified certificates issued to legal persons offering the level of quality defined in [Law (46) 2021] for UAE qualified certificates and requiring the use of a UAE Qualified Seal Creation Device (QSCD). The identifier for this policy is: 2.16.784.1.1.8.1.4
   The requirements applicable to the services offered under one of those certificate policies are indicated by clauses marked by the applicable certificate policy indicator: "[UAE-QCP-l]", "[UAE-QCP-n]", "[UAE-QCP-l-qscd]" and/or "[UAE-QCP-n-qscd]"
   The requirements applicable to any CP are indicated by clauses without any additional marking.

6.2 General requirements

GPR-1	Qualified certificates for electronic signature not intended to support the creation of qualified electronic signatures shall be issued under the [UAE-QCP-n] requirements.
GPR-2	Qualified certificates for electronic seal not intended to support the creation of qualified electronic seals shall be issued under the [UAE-QCP-l] requirements.
GPR-3	Qualified certificates for electronic signature intended to support the creation of qualified electronic signatures shall be issued under the [UAE-QCP-n-qscd] requirements.

GPR-4	Qualified certificates for electronic seal intended to support the creation of qualified electronic seals shall be issued under the [UAE-QCP-l-qscd] requirements.
GPR-5	[UAE-QCP-n]: All requirements defined in [ETSI EN 319 411-2] for the certificate policy [QCP-n] shall apply with the amendments provided in the subsequent clauses of the present section, which shall prevail over the corresponding requirements of the former.
GPR-6	[UAE-QCP-l]: All requirements defined in [ETSI EN 319 411-2] for the certificate policy [QCP-l] shall apply with the amendments provided in the subsequent clauses of the present section, which shall prevail over the corresponding requirements of the former.
GPR-7	[UAE-QCP-n-qscd]: All requirements defined in [ETSI EN 319 411-2] for the certificate policy [QCP-n-qscd] shall apply with the amendments provided in the subsequent clauses of the present section, which shall prevail over the corresponding requirements of the former.
GPR-8	[UAE-QCP-l-qscd]: All requirements defined in [ETSI EN 319 411-2] for the certificate policy [QCP-l-qscd] shall apply with the amendments provided in the subsequent clauses of the present section, which shall prevail over the corresponding requirements of the former.
GPR-9	References made in [ETSI EN 319 411-2] to [ETSI EN 319 411-1] shall be understood as referring to the version of that standard amended according to section 3 “Specific provisions for trust service providers issuing certificates for electronic signatures and/or certificates for electronic seals” of the present document.
GPR-10	References made in [ETSI EN 319 411-2] to "(EU) advanced electronic signatures" and "(EU) advanced electronic seal" are replaced respectively by references to advanced electronic signatures and to advanced electronic seals as defined in [Law (46) 2021].
GPR-11	References made in [ETSI EN 319 411-2] to "(EU) qualified electronic signatures" and "(EU) qualified electronic seal" are replaced respectively by references to qualified electronic signatures and to qualified electronic seals as defined in [Law (46) 2021].
GPR-12	Requirements stated in [ETSI EN 319 411-2] as applicable to "EU qualified certificates" shall apply mutatis mutandis to qualified certificates issued under [Law (46) 2021].
GPR-13	References made in [ETSI EN 319 411-2] to “eIDAS Regulation (EU) No 910/2014" are replaced by references to [Law (46) 2021].

6.3 Issuance, management and revocation of qualified certificates

CCY-1	The QTSP shall proceed to the registration, the management and the revocation of qualified certificates in conformance with [ETSI EN 319 411-2], in particular with its clauses 6.1, 6.2, and 6.3, with the following amendments: a. Once a qualified certificate is activated or accepted whichever event comes first, the QTSP shall not proceed to the suspension of the certificate. b. With regards to the identity verification referred to in paragraph 1 of Article (34) of [Law (46) 2021]: (i) The QTSP shall verify that the subscriber is the sole claimant of the identity being claimed

(ii) The QTSP shall check the accuracy and legitimacy of the identification data provided by the subscriber. This include checking that subscriber's email address and/or mobile number exist(s) and is(are) under subscriber's control.

(iii) The QTSP shall verify primary & secondary pieces of evidence, in accordance with the UAE laws and with an authoritative source (e.g. issuing authority). Primary evidence are defined as government issued secure photo ID evidence types with robust identity proofing, issuance and management processes. Secondary evidence are evidence types from government or non-government sources that are supported by moderate identity proofing, issuance and management processes.

(iv) One of the pieces of evidence referred to in (iii) shall be a valid and genuine passport, a valid and genuine UAE identity card or a valid and genuine identity card recognised to give access to the UAE territory. The QTSP shall verify that the presented evidences do not seem forged or counterfeit and do not show signs of falsification. This shall be done using the PRADO register and guidelines available from www.consilium.europa.eu/prado.

(v) The QTSP shall verify with an UAE federal or national authoritative source that the identity of the subscriber is not that of a deceased person (individual) or of a terminated person (organization/corporation)

(vi) The QTSP shall verify the link between the claimed identity and the claimant subscriber, during an in-person interview or through an equivalent method, via one of the following methods:

- Manual comparison of person's face against photo on primary document. This verification must confirm that the person's face corresponds to the photo on the primary evidence authenticated document.
- Verification of a biometric previously collected;
- Knowledge based authentication.

(vii) The QTSP shall check the collected identification information with information held within the national or relevant organization of known fraudulent identities (e.g. police, law enforcement, government agencies) and with authoritative sources used in (iii). In particular, the presented primary and secondary evidences shall be verified not having been reported lost, stolen or revoked by the relevant authoritative source.

(viii) The QTSP shall verify that the content of the qualified certificate they issue are not in contradiction with those data of relevant authoritative sources, in particular with Federal or National Trade Registers with regards to identification data related to legal person, and data regarding the association between a natural person and a legal person.

	(ix) The QTSP may accept electronic identification tools that are listed in the TDRA register of approved electronic identification tools provided they are listed: - as meeting the requirements providing a high level of assurance with regards to the identity of the person to whom the qualified certificate is issued, and - as requiring the physical presence of the requestor as a pre-requisite to the delivery of the electronic identification tool. (x) The QTSP may use qualified certificates supporting a qualified electronic signature or a qualified electronic seal for the verification of the identity prior the delivery of a qualified certificate for electronic signature or of a qualified certificate for electronic seal respectively. In that case: - the qualified electronic signature or qualified electronic seal must have been created on the electronic document used to request the new qualified certificate and including all the required information for the delivery of the certificate, - the QTSP must implement a process for the validation of the qualified electronic signature or qualified electronic seal in accordance with [Law (46) 2021] or make use of a qualified validation service for the validation of qualified electronic signature or qualified electronic seal in accordance with [Law (46) 2021] (xi) The QTSP may use any other identification procedure provided: - it is confirmed by an accredited CAB that the implementation of that procedure by the QTSP provides equivalent assurance in terms of reliability to physical presence; - this confirmation must demonstrates the implementation of technical and organizational measures mitigating the risks of fraud and impersonation with an efficiency at least equivalent to physical presence, and mitigating the risks related to the tampering, fraudulent manipulation or handling of communication channels (including audio and video communications); - the procedure is verified and approved by TDRA or its delegate prior its implementation in production.
CCY-2	REG-6.2.3-01 of [ETSI EN 319 411-2] is amended so it reads: “The requirements identified in ETSI EN 319 411-1 [2], clause 6.2.3 and clauses (ix), (x) and (xi) of the requirement CCY-1 shall apply.”

6.4 Content profile for qualified certificates for electronic signatures

PSI-1	Qualified certificates for electronic signatures shall conform to [ETSI EN 319 412-2] as amended in section 3.5 “Content profile for certificates for electronic signatures” with the following additional requirements: a. Qualified certificates for electronic signatures shall include QCStatements in accordance with [ETSI EN 319 412-5]. b. Qualified certificates for electronic signatures shall include the qualified electronic signature or qualified electronic seal of the issuing qualified trust service provider; NOTE: This is compatible with requirement **PSI-1** of section 3.5 “Content profile for certificates for electronic signatures” which requires the presence of the advanced electronic signature or advanced electronic seal of the issuing trust service provider. c. The value of the organizationIdentifier attribute shall be structured as follows: NTRAE-AuthCode.TradeLicence where "AuthCode" is an alphanumeric code allocated to the UAE federal, national or local Trade Licensing Authority and "TradeLicence" is a numeric trade license identifier allocated to the organization by the national or local Trade Licensing Authority identified by "AuthCode". d. Where the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device, this shall be indicated in qualified certificates for electronic signatures by means of the QcSSCD statement as described in clause 4.2.2 of [ETSI EN 319 412-5]. e. The policy identifiers defined in clause 5.3 of [ETSI EN 319 411-2] (i.e. QCP-n, QCP-n-qscd) shall not be included in end-entity certificates). f. When certificates are issued as UAE Qualified Certificates, they shall include one of the OIDs corresponding to the certificate policies defined in section 6.1 of the present document.

6.5 Content profile for qualified certificates for electronic seals

PSE-1	All certificate fields and extensions shall comply with [ETSI EN 319 412-3] with the amendments specified in the present document. All references to [ETSI EN 319 412-2] made in [ETSI EN 319 412-3] shall be understood as referring to the version amended according to section 6.4 “Content profile for qualified certificates for electronic signatures” of the present document.
PSE-2	Qualified certificates for electronic seals shall conform to [ETSI EN 319 412-3] to the exception of clause 5 and with the following amendments: a. Qualified certificates for electronic signatures shall include QCStatements in accordance with [ETSI EN 319 412-5]. b. Qualified certificates for electronic seals shall include the qualified electronic signature or qualified electronic seal of the issuing qualified trust service provider;

	NOTE: This is compatible with requirement **PSE-1** of section 3.6 “Content profile for certificates for electronic seals” which requires the presence of the advanced electronic signature or advanced electronic seal of the issuing trust service provider. c. The value of the organizationIdentifier attribute included in the identity of the subject shall be structured as follows: NTRAE-AuthCode.TradeLicence where "AuthCode" is an alphanumeric code allocated to the UAE federal, national or local Trade Licensing Authority and "TradeLicence" is a numeric trade license identifier allocated to the organization by the national or local Trade Licensing Authority identified by "AuthCode". d. Where the electronic seal creation data related to the electronic seal validation data is located in a qualified electronic seal creation device, this shall be indicated in qualified certificates for electronic seals by means of the QcSSCD statement as described in clause 4.2.2 of [ETSI EN 319 412-5]. e. The policy identifiers defined in clause 5.3 of [ETSI EN 319 411-2] (i.e. QCP-l, QCP-l-qscd) shall not be included in the certificate. f. When certificates are issued as UAE Qualified Certificates, they shall include one of the OIDs corresponding to the certificate policies defined in section 6.1 of the present document.

6.6 Provisions related to the inclusion of the related qualified trust service in the UAE trusted list

TL-1	A QTS consisting in the issuance of qualified certificates is identified in the UAE trusted list by means of an electronic certificate of root-CA, an intermediate CA or an issuing CA.
TL-2	The confirmation by an accredited CAB and the verification by TDRA of the conformity of the QTSP and the QTS it provides with the requirements of [Law (46) 2021] and of the applicable TDRA resolutions must allow the demonstration that under the CA identified in **TL-1** above, it is possible to distinguish without any ambiguity qualified certificates from non-qualified certificates, and qualified certificates for electronic signatures from qualified certificates for electronic seals.
TL-3	The QTSP shall not include in non-qualified certificates any data or attribute that might lead to identify them erroneously as qualified.

7 Specific provisions for qualified trust service providers issuing qualified time stamps

7.1 General requirements

GPR-1	The QTSP issuing qualified time stamps shall conform to [ETSI EN 319 421] and [ETSI EN 319 422] with the amendments provided in the subsequent articles of the present document, which have precedence on specifications from [ETSI EN 319 421] and [ETSI EN 319 422].
GPR-2	References made in [ETSI EN 319 421] and [ETSI EN 319 422] to [ETSI EN 319 401] shall be understood as referring to the version of that standard as indicated in [ETSI EN 319 401] and amended according to section 2 “General provisions for all trust services provided by a trust service provider” of the present document.
GPR-3	References made in [ETSI EN 319 421] and [ETSI EN 319 422] to "(EU) advanced electronic signatures" and "(EU) advanced electronic seal" are replaced respectively by references to advanced electronic signatures and to advanced electronic seals as defined in [Law (46) 2021].
GPR-4	References made in [ETSI EN 319 421] and [ETSI EN 319 422] to "(EU) qualified electronic signatures" and "(EU) qualified electronic seal" are replaced respectively by references to qualified electronic signatures and to qualified electronic seals as defined in [Law (46) 2021].
GPR-5	Requirements stated in [ETSI EN 319 421] and [ETSI EN 319 422] as applicable to "EU qualified certificates" shall apply mutatis mutandis to qualified certificates issued under [Law (46) 2021].
GPR-6	References made in [ETSI EN 319 421] and [ETSI EN 319 422] to “eIDAS Regulation (EU) No 910/2014" are replaced by references to [Law (46) 2021].

7.2 Time stamping policy and time stamping practice statement

TPS-1	The QTSP issuing (qualified) time stamps shall specify and maintain the set of policies and practices appropriate for the issuance of time stamps it provides as a qualified trust service under the form of time stamping policies and time stamping practice statement (TSAPS) in conformance with [ETSI EN 319 421] provided: a. The QTSP's time stamping policies and TSAPS shall be structured in accordance with [ETSI EN 319 421]. b. The QTSP's time stamping policies and TSAPS shall be identified by means of unique object identifiers of the form required in Recommendation ITU-T [X.509]. The policy identifier of the applicable policy shall be included in the time stamps issued in accordance with that policy. c. The QTSP shall publicly disclose its time stamping policies, its TSAPS, and their revisions through an online means that is available on a 24x7 basis. d. The QTSP shall publish TSA Disclosure Statement(s) (TDS) that summarize key points of its time stamping policy(ies) for the benefit of subscribers and relying parties.

	e. The TSA Disclosure Statement(s) (TDS) shall be structured in accordance with Annex B of [ETSI EN 319 421]. f. The QTSP shall publish an English translation of its TSAPS, time stamping policies and TDS(s).
TPS-2	The QTSP shall retain overall responsibility for the provision of the QTS it provides and for conformance with the procedures prescribed in its practices and its time stamping policies or the time stamping policies it supports, even when the QTSP's functionality, or part of it, is undertaken by outsourcers. To this extent, the QTSP shall define the outsourcers' liability and ensure that outsourcers are bound to implement any controls required by the QTSP.

7.3 Issuance and management of (qualified) time stamps

TST-1	The time stamping provisioning system used by the QTSP to issue time stamps should be certified against [CEN TS 419 261] and [CEN EN 419 231].

7.4 Provisions related to the inclusion of the related qualified trust service in the UAE trusted list

TL-1	A QTS consisting in the issuance of qualified time stamps is identified in the UAE trusted list by means of a qualified certificate of: a. a TSU, b. an issuing CA, operated by the QTSP, only for its own use, issuing only certificates for electronic signatures or for electronic seals that shall only be used for creating advanced electronic signatures or advanced electronic seals on qualified electronic time stamps issued by the QTSP.
TL-2	In case of **TL-1** clause (a) above, as many services shall be included in the UAE trusted list as there are TSUs used by the QTSP.
TL-3	In case of **TL-1** clause (b) above, the confirmation by an accredited CAB and the verification by TDRA of the conformity of the QTSP and the QTS it provides with the requirements of [Law (46) 2021] and of the applicable TDRA resolutions must demonstrate that the issuing CA meet these requirements.
TL-4	The QTSP shall not issue any data object that might be interpreted as qualified time-stamps when those data objects do not meet the requirements for qualified time-stamps laid down in the [Law (46) 2021].

8 Specific provisions for qualified trust service providers providing qualified preservation of qualified electronic signature and qualified electronic seal

8.1 General requirements

GPR-1	The QTSP providing qualified preservation services for QESig and/or QESeal shall conform to [ETSI TS 119 511] and [ETSI TS 119 512] with the amendments provided in the subsequent articles of the present document, which have precedence on specifications from [ETSI TS 119 511] and [ETSI TS 119 512].
GPR-2	The preservation goal of the QTSP's qualified preservation service shall be the "Preservation of Electronic Signatures" defined in clause 4.2 [ETSI TS 119 512]. NOTE: The requirements corresponding to that goal are tagged as [PDS] in [ETSI TS 119 511].
GPR-3	References made in [ETSI TS 119 511] and [ETSI TS 119 512] to [ETSI EN 319 401] shall be understood as referring to the version of that standard as indicated in [ETSI EN 319 401] and amended according to section 2 "General provisions for all trust services provided by a trust service provider" of the present document.
GPR-4	References made in [ETSI TS 119 511] and [ETSI TS 119 512] to "(EU) advanced electronic signatures" and "(EU) advanced electronic seal" are replaced respectively by references to advanced electronic signatures and to advanced electronic seals as defined in [Law (46) 2021].
GPR-5	References made in [ETSI TS 119 511] and [ETSI TS 119 512] to "(EU) qualified electronic signatures" and "(EU) qualified electronic seal" are replaced respectively by references to qualified electronic signatures and to qualified electronic seals as defined in [Law (46) 2021].
GPR-6	Requirements stated in [ETSI TS 119 511] and [ETSI TS 119 512] as applicable to "EU qualified certificates" shall apply mutatis mutandis to qualified certificates issued under [Law (46) 2021].
GPR-7	References made in [ETSI TS 119 511] to "EUMS trusted list" shall be understood as references to UAE trusted list.
GPR-8	References made in [ETSI TS 119 511] and [ETSI TS 119 512] to "eIDAS Regulation (EU) No 910/2014" are replaced by references to [Law (46) 2021].

8.2 Preservation policies / Preservation service practice statement

PPS-1	The QTSP providing qualified preservation services for QESig and/or QESeal shall specify and maintain the set of policies and practices appropriate for the qualified preservation service it provides under the

	form of preservation service policies and preservation service practice statement (PSPS) in conformance with [ETSI TS 119 511] provided: a. The QTSP's preservation service policies and preservation evidence policies (hereafter preservation policies) and PSPS shall be established and structured in accordance with [ETSI TS 119 511]. The preservation evidence policy shall be included directly or by reference in the preservation evidence. If the preservation evidence policy is included in the preservation evidence, it shall be cryptographically protected. b. The QTSP's preservation policies and PSPS shall be identified by means of unique object identifiers of the form required in Recommendation ITU-T X.509 [X.509]. c. The QTSP shall publicly disclose its preservation policies, its PSPS, and their revisions through an online means that is available on a 24x7 basis. d. The QTSP shall publish preservation service Disclosure Statement(s) (PSDS) that summarize key points of its preservation policy(ies) for the benefit of subscribers and relying parties. e. The QTSP shall publish an English translation of its PSPS, preservation policies and PSDS(s).
PPS-2	The QTSP shall retain overall responsibility for the provision of the QTS it provides and for conformance with the procedures prescribed in its practices and its preservation policies or the preservation policies it supports, even when the QTSP's functionality, or part of it, is undertaken by outsourcers. To this extent, the QTSP shall define the outsourcers' liability and ensure that outsourcers are bound to implement any controls required by the QTSP.
PPS-3	The QTS shall preserve all information needed to check the qualification status of the electronic signature or seal that would not be publicly available until the end of the preservation period.

8.3 Issuance and management of qualified preservation evidences

CCY-1	The preservation service trustworthy systems used by the QTSP to provide qualified preservation services should be certified against an appropriate standard or protection profile.
CCY-2	[RFC 3161] time-stamps added by the QTSP within the preservation evidence shall be qualified electronic time stamps conformant with [Law (46) 2021].

8.4 Termination

TER-1	In addition to OVR-7.12-02 [WST] of [ETSI TS 119 511]:

	a. The QTSP must provide for transfer procedures to ensure the integrity and operability of all preservation objects (POs), either to the original applicant or to another QTSP providing qualified preservation service for QESig/QESeal with the express agreement of the original applicant. b. These elements shall be legible and understandable by the recipient, and must be in a format that allows them to be used correctly. c. The reliability of qualified electronic signatures and/or qualified electronic seals shall not be affected by this transfer. d. The QTSP may refuse the qualified preservation of qualified electronic signatures or qualified electronic seals provided in proprietary formats, if it considers that it is not possible for it to be legible in time, and provided the applicant/subscriber is duly informed before subscribing to the service.

8.5 Provisions related to the inclusion of the related qualified trust service in the UAE trusted list

TL-1	The QTSP shall have for each instance of the preservation service it provides, one service digital identifier as defined in clause 5.5.3 of [ETSI TS 119 612] which allows to uniquely and unambiguously identify the service within the UAE trusted list as specified hereafter.
TL-2	A QTS consisting in the provisioning of qualified preservation service for QESig/QESeal is identified in the UAE trusted list by means of: a. a digital certificate of the QTSP, corresponding to the private key used to sign or seal preservation service evidences or acknowledgment receipt of preservation requests, b. a certificate of an issuing CA, operated by the QTSP, only for the use of the QTSP providing qualified preservation services, issuing only certificates for electronic signatures or for electronic seals that shall only be used for creating advanced electronic signatures or advanced electronic seals on qualified preservation service evidences, or acknowledgment receipt of preservation requests, issued by the QTSP. c. In case no PKI public key technology is used to identify the preservation QTS, an indicator expressed by a URI which uniquely and unambiguously identifies the preservation service.
TL-3	In case of TL-2 clause (a) above, as many services shall be included in the UAE trusted list as there are private/public key pairs used by the QTSP.
TL-4	In case of TL-2 clause (b) above, the confirmation by an accredited CAB and the verification by TDRA of the conformity of the QTSP and the QTS it provides with the requirements of [Law (46) 2021] and of the applicable TDRA resolutions must demonstrate that the issuing CA meets these requirements.

TL-5	The QTSP shall not issue any data object that might be interpreted as (qualified) preservation evidences when those data objects do not meet the requirements for (qualified) preservation evidences laid down in the [Law (46) 2021].

9 Specific provisions for qualified trust service providers providing qualified validation of qualified electronic signature and qualified electronic seal

9.1 General requirements

GPR-1	The QTSP providing qualified validation services for QESig and/or QESeal shall conform to [ETSI TS 119 441], excluding its Annex B, and [ETSI TS 119 442] with the amendments provided in the subsequent articles of the present document, which have precedence on specifications from [ETSI TS 119 441] and [ETSI TS 119 442].
GPR-2	References made in [ETSI TS 119 441] and [ETSI TS 119 442] to [ETSI EN 319 401] shall be understood as referring to the version of that standard as indicated in [ETSI EN 319 401] and amended according to section 2 “General provisions for all trust services provided by a trust service provider” of the present document.
GPR-3	References made in [ETSI TS 119 441] and [ETSI TS 119 442] to "(EU) advanced electronic signatures" and "(EU) advanced electronic seal" are replaced respectively by references to advanced electronic signatures and to advanced electronic seals as defined in [Law (46) 2021].
GPR-4	References made in [ETSI TS 119 441] and [ETSI TS 119 442] to "(EU) qualified electronic signatures" and "(EU) qualified electronic seal" are replaced respectively by references to qualified electronic signatures and to qualified electronic seals as defined in [Law (46) 2021].
GPR-5	Requirements stated in [ETSI TS 119 441] and [ETSI TS 119 442] as applicable to "EU qualified certificates" shall apply mutatis mutandis to qualified certificates issued under [Law (46) 2021].
GPR-6	References made in [ETSI TS 119 441] to "EUMS trusted list" shall be understood as references to UAE trusted list.
GPR-7	References made in [ETSI TS 119 441] and [ETSI TS 119 442] to “eIDAS Regulation (EU) No 910/2014" are replaced by references to [Law (46) 2021].

9.2 Validation service policy / validation service practice statement

VPS-1	The QTSP providing qualified validation services for QESig and/or QESeal shall specify and maintain the set of policies and practices appropriate for the qualified validation service it provides under the form of validation service policies and validation service practice statement (VSPS) in conformance with [ETSI TS 119 441], provided: a. The QTSP's validation service policies and VSPS shall be structured in accordance with [ETSI TS 119 441] and in particular with its Annexure A.

	b. The QTSP's validation service policies and VSPS shall be identified by means of unique object identifiers of the form required in Recommendation ITU-T [X.509]. c. The QTSP shall publicly disclose its validation service policies, its VSPS, and their revisions through an online means that is available on a 24x7 basis. d. The QTSP shall publish validation service Disclosure Statement(s) (VSDS) that summarize key points of its validation service policy(ies) for the benefit of subscribers and relying parties. e. The QTSP shall publish an English translation of its VSPS, validation service policies and VSDS(s).
VPS-2	The QTSP shall retain overall responsibility for the provision of the QTS it provides and for conformance with the procedures prescribed in its practices and its validation service policies or the validation service policies it supports, even when the QTSP's functionality, or part of it, is undertaken by outsourcers. To this extent, the QTSP shall define the outsourcers' liability and ensure that outsourcers are bound to implement any controls required by the QTSP.
VPS-3	Time-stamps added by the QTSP within the validation report shall be qualified time stamps.

9.3 Facility, Management, Operational and Security Controls

OPS-1	The validation service provided as a QTS by the QTSP shall conform to the [TL onboarding guide for third parties].
OPS-2	The QTSP shall test its service to demonstrate the correct implementation of OPS-1 and shall describe such tests in its practice statements.
OPS-3	The tests referred to in OPS-2 shall check different use-cases, positive and negative ones and be sufficient in quantity and quality to provide significant evidence of the conformance of the service.
OPS-4	The validation service provided as a QTS by the QTSP shall permit relying parties to receive validation result of the qualified electronic signature/seal in an automated, reliable and efficient manner that can be processed by a machine. Complying with [ETSI TS 119 442] and with [ETSI TS 119 102-2] will provide a presumption of compliance with this requirement.
OPS-5	When the validation report is presented through a webpage, the website and the QTSP shall be authenticated within a TLS session.
OPS-6	When an [RFC 3161] time stamp is present in the validated QESig/QESeal, the validation report shall report if the [RFC 3161] time stamp is a qualified electronic time-stamp as per [Law (46) 2021].
OPS-7	The validation report shall conform to [ETSI TS 119 102-2].

OPS-8	The information requested by SVR-8.4-08 andSVR-8.4-09 of [ETSI TS 119 441] shall be under the form of a certificate that bears the name of the QTSP such as indicated in the official reports.
OPS-9	The QTSP shall control the hash computation (either perform the computation on the server side or control the client if it is allowed on the client side).
OPS-10	The validation service policy shall clearly be identified as a validation policy for validating that a signature is a qualified electronic signature or seal as per [Law (46) 2021].
OPS-11	The validation report shall indicate whether the electronic signature is a qualified electronic signature or a qualified electronic seal as per [Law (46) 2021].
OPS-12	The validation report shall allow the relying party to detect any security relevant issues.
OPS-13	The validation service trustworthy systems used by the QTSP to provide qualified validation services should be certified against an appropriate standard or protection profile.
OPS-14	[RFC 3161] time stamps added by the QTSP within the validation report shall be qualified time stamps.
OPS-15	The validation report shall bear the advanced electronic signature or advanced electronic seal of the QTSP.

9.4 Provisions related to the inclusion of the related qualified trust service in the UAE trusted list

TL-1	The QTSP shall have for each instance of the validation service it provides, one service digital identifier as defined in clause 5.5.3 of [ETSI TS 119 612] which allows to uniquely and unambiguously identify the service within the UAE trusted list as specified hereafter.
TL-2	A QTS consisting in the provisioning of qualified validation service for QESig/QESeal is identified in the UAE trusted list by means of: a. a digital certificate of the QTSP, corresponding to the private key used to create advanced electronic signatures or seals on validation service evidences (reports), b. a certificate of an issuing CA, operated by the QTSP, only for its own use, issuing only certificates for electronic signatures or for electronic seals that shall only be used for creating advanced electronic signatures or advanced electronic seals on qualified validation service evidences (reports) issued by the QTSP.
TL-3	In case of **TL-2** clause (a) above, as many services shall be included in the UAE trusted list as there are private/public key pairs used by the QTSP.

TL-4	In case of **TL-2** clause (b) above, the confirmation by an accredited CAB and the verification by TDRA of the conformity of the QTSP and the QTS it provides with the requirements of [Law (46) 2021] and of the applicable TDRA resolutions must demonstrate that the issuing CA meet these requirements.
TL-5	The QTSP shall not issue any validation report that might be interpreted as being the result of a process for the qualified validation of qualified electronic signature or seal when those validation reports are not the result of a validation process that meets the requirements for the qualified validation for electronic signature or seal laid down in the [Law (46) 2021].

10 Specific provisions for qualified trust service providers providing management of remote Qualified signatures and remote qualified seals creation devices as a qualified trust service

10.1 General requirements

GPR-1	The QTSP providing management of remote QSCD as a QTS shall conform to [ETSI EN 319 401] and to [ETSI TS 119 431-1] in particular with its Annex A for the QTS it provides with the amendments provided in the subsequent articles of the present document, which have precedence on specifications from [ETSI TS 119 431-1].
GPR-2	References made in [ETSI TS 119 431-1] to [ETSI EN 319 401] shall be understood as referring to the version of the corresponding standard as indicated in [ETSI EN 319 401] and amended according to section 2 “General provisions for all trust services provided by a trust service provider” of the present document.
GPR-3	References made in [ETSI TS 119 431-1] to [ETSI EN 319 411-1] shall be understood as referring to the version of the corresponding standard as indicated in [ETSI EN 319 411-1] and amended according to section 3 of the present document.
GPR-4	References made in [ETSI TS 119 431-1] to "(EU) advanced electronic signatures" and "(EU) advanced electronic seal" are replaced respectively by references to advanced electronic signatures and to advanced electronic seals as defined in [Law (46) 2021].
GPR-5	References made in [ETSI TS 119 431-1] to "(EU) qualified electronic signatures" and "(EU) qualified electronic seal" are replaced respectively by references to qualified electronic signatures and to qualified electronic seals as defined in [Law (46) 2021].
GPR-6	References made in [ETSI TS 119 431-1] to “eIDAS Regulation (EU) No 910/2014" are replaced by references to [Law (46) 2021].
GPR-7	Requirements stated in [ETSI TS 119 431-1] as applicable to "EU qualified certificates" shall apply mutatis mutandis to qualified certificates issued under [Law (46) 2021].
GPR-8	References made in [ETSI TS 119 431-1] to "EUMS trusted list" shall be understood as references to “UAE trusted list”.

10.2 Trust service policy and trust service practice statement

TPS-1	The QTSP providing management of remote QSCD as a QTS shall specify and maintain the set of policies and practices appropriate for the QTS it provides under the form of QTS policies and QTS practice statement (QTSPS) in conformance with [ETSI TS 119 431-1], provided:

	a. The QTSP's QTS policies and QTSPS shall be established and structured in accordance with [ETSI TS 119 431-1]. b. The QTSP's QTS policies and QTSPS shall be identified by means of unique object identifiers of the form required in Recommendation ITU-T [X.509]. c. The QTSP shall publicly disclose its QTS policies, its QTSPS, and their revisions through an online means that is available on a 24x7 basis. d. The QTSP shall publish QTS Disclosure Statement(s) (QTSDS) that summarize key points of its QTS policy(ies) for the benefit of subscribers and relying parties. e. The QTSP shall publish an English translation of its QTSPS, QTS policies and QTSDS(s).
TPS-2	The QTSP shall retain overall responsibility for the provision of the QTS it provides and for conformance with the procedures prescribed in its practices and its trust service policies or the trust service policies it supports, even when the QTSP's functionality, or part of it, is undertaken by outsourcers. To this extent, the QTSP shall define the outsourcers' liability and ensure that outsourcers are bound to implement any controls required by the QTSP.

10.3 Facility, Management, Operational and Security Controls

OPS-1	The trustworthy systems used by the QTSP to provide management of remote QSCD as a QTS should be certified against ETSI TS 119 431-1.

10.4 Provisions related to the inclusion of the related qualified trust service in the UAE trusted list

TL-1	The QTSP shall have for each instance of the management of remote QSCD as a QTS it provides, one service digital identifier as defined in clause 5.5.3 of [ETSI TS 119 612] which allows to uniquely and unambiguously identify the service within the UAE trusted list as specified hereafter.
TL-2	In case no PKI public key technology is used to identify a QTS consisting in the provisioning of management of remote QSCD as a QTS, the QTS is identified in the UAE trusted list by means of an indicator expressed by a URI which uniquely and unambiguously identifies the QTS.

11 Specific provisions for qualified trust service providers providing local qualified signatures and local qualified seals creation devices as a qualified trust service

11.1 General requirements

GPR-1	The QTSP providing local QSCD as a QTS shall conform to [ETSI EN 319 401] and the relevant parts of [ETSI EN 319 411-2] with the amendments provided in the subsequent articles of the present document, which have precedence on those specifications.
GPR-2	References made in [ETSI EN 319 411-2] to [ETSI EN 319 401] shall be understood as referring to the version of the corresponding standard as indicated in [ETSI EN 319 401] and amended according to section 2 “General provisions for all trust services provided by a trust service provider” of the present document.
GPR-3	References made in [ETSI EN 319 411-2] to [ETSI EN 319 411-1] shall be understood as referring to the version of the corresponding standard as indicated in [ETSI EN 319 411-1] and amended according to section 3 “Specific provisions for trust service providers issuing certificates for electronic signatures and/or certificates for electronic seals” of the present document.
GPR-4	References made in [ETSI EN 319 411-2], [ETSI EN 319 411-1] or [ETSI EN 319 401] to "(EU) advanced electronic signatures" and "(EU) advanced electronic seal" are replaced respectively by references to advanced electronic signatures and to advanced electronic seals as defined in [Law (46) 2021].
GPR-5	References made in [ETSI EN 319 411-2], [ETSI EN 319 411-1] or [ETSI EN 319 401] to "(EU) qualified electronic signatures" and "(EU) qualified electronic seal" are replaced respectively by references to qualified electronic signatures and to qualified electronic seals as defined in [Law (46) 2021].
GPR-6	References made in [ETSI EN 319 411-2], [ETSI EN 319 411-1] or [ETSI EN 319 401] to eIDAS Regulation (EU) No 910/2014 are replaced by references to [Law (46) 2021].
GPR-7	Requirements stated in [ETSI EN 319 411-2], [ETSI EN 319 411-1] or [ETSI EN 319 401] as applicable to "EU qualified certificates" shall apply mutatis mutandis to qualified certificates issued under [Law (46) 2021].
GPR-8	References made in in [ETSI EN 319 411-2], [ETSI EN 319 411-1] or [ETSI EN 319 401] to "EUMS trusted list" shall be understood as references to UAE trusted list.

11.2 Trust service policy and trust service practice statement

TPS-1	The QTSP providing local QSCD as a QTS shall specify and maintain the set of policies and practices appropriate for the QTS it provides under the form of QTS policies and QTS practice statement (QTSPS) in conformance with the requirements of section 11.1 provided: a. The QTSP's QTS policies and QTSPS shall be identified by means of unique object identifiers of the form required in Recommendation ITU-T [X.509]. b. The QTSP shall publicly disclose its QTS policies, its QTSPS, and their revisions through an online means that is available on a 24x7 basis. c. The QTSP shall publish QTS Disclosure Statement(s) (QTSDS) that summarize key points of its QTS policy(ies) for the benefit of subscribers and relying parties. d. The QTSP shall publish an English translation of its QTSPS, QTS policies and QTSDS(s).
TPS-2	The QTSP shall retain overall responsibility for the provision of the QTS it provides and for conformance with the procedures prescribed in its practices and its trust service policies or the trust service policies it supports, even when the QTSP's functionality, or part of it, is undertaken by outsourcers. To this extent, the QTSP shall define the outsourcers' liability and ensure that outsourcers are bound to implement any controls required by the QTSP.

11.3 Provisions related to the inclusion of the related qualified trust service in the UAE trusted list

TL-1	The QTSP shall have for each instance of the provision of local QSCD as a QTS it provides, one service digital identifier as defined in clause 5.5.3 of [ETSI TS 119 612] which allows to uniquely and unambiguously identify the service within the UAE trusted list as specified hereafter.
TL-2	In case no PKI public key technology is used to identify a QTS consisting in the provisioning of local QSCD as a QTS, the QTS is identified in the UAE trusted list by means of an indicator expressed by a URI which uniquely and unambiguously identifies the QTS.

12 Specific provisions for qualified trust service providers providing qualified electronic delivery services

12.1 General requirements

GPR-1	The QTSP providing qualified electronic delivery services shall conform to the requirements applicable to “EU QERDSP” in [ETSI EN 319 521] and to [ETSI EN 319 522 (all parts)] with the amendments provided in the subsequent clauses of the present document, which shall prevail over the corresponding requirements of the former.
GPR-2	References made in [ETSI EN 319 521] and in [ETSI EN 319 522 (all parts)] to ETSI EN 319 401 shall be understood as referring to the version of that standard amended according to section 2 “General provisions for all trust services provided by a trust service provider” of the present document.
GPR-3	References made in [ETSI EN 319 521] and in [ETSI EN 319 522 (all parts)] to ETSI EN 319 411-1 shall be understood as referring to the version of that standard amended according to section 3 “Specific provisions for trust service providers issuing certificates for electronic signatures and/or certificates for electronic seals” of the present document.
GPR-4	All mention of "EU qualified certificates" in [ETSI EN 319 521] and in [ETSI EN 319 522 (all parts)] shall read "UAE qualified certificates".
GPR-5	All mention of "Regulation (EU) No 910/2014" in [ETSI EN 319 521] and in [ETSI EN 319 522 (all parts)] shall read "[Law (46) 2021]".
GPR-6	All mention of “(EU) qualified electronic signatures” and “(EU) qualified electronic seal” in [ETSI EN 319 521] and in [ETSI EN 319 522 (all parts)] shall read respectively as “UAE qualified electronic signatures” and “UAE qualified electronic seals” as defined in [Law (46) 2021].
GPR-7	All mention of "EU QERDS" and “EU QERDSP” in [ETSI EN 319 521] and in [ETSI EN 319 522 (all parts)] shall read respectively as “UAE qualified electronic delivery services” and “UAE qualified trust service provider providing qualified electronic delivery services” as defined in [Law (46) 2021].
GPR-8	All mention of “qualified time seal”, “qualified service”, “qualified status”, and “qualified trust service provider” in [ETSI EN 319 521] and in [ETSI EN 319 522 (all parts)] shall be understood as the same concepts defined in [Law (46) 2021].
GPR-9	All mention of “qualified electronic registered delivery services” in [ETSI EN 319 521] and [ETSI EN 319 522 (all parts)] shall read as “qualified electronic delivery services” as defined in [Law (46) 2021].
GPR-10	All mention of “EUMS trusted list” in [ETSI EN 319 521] and in [ETSI EN 319 522 (all parts)] shall read as “UAE trusted list” as defined in [Law (46) 2021].

12.2 Electronic delivery service policy and practice statement

VPS-1	The QTSP's electronic delivery service policies and practice statement(s) shall be structured in accordance with [ETSI EN 319 521].
VPS-2	The QTSP's electronic delivery service policies and practice statement(s) shall be identified by means of unique object identifiers of the form required in Recommendation [X.509].
VPS-3	The QTSP shall publicly disclose its electronic delivery service policies, practice statement(s), and their revisions through an online means that is available on a 24x7 basis.
VPS-4	The QTSP shall publish an electronic delivery service Disclosure Statement(s) that summarize key points of its validation service policy(ies) for the benefit of subscribers and relying parties.
VPS-5	The QTSP shall publish an English translation of its electronic delivery service policies, practice statement(s) and disclosure statemen(s).

12.3 ERD messages and ERDS evidences

RDS-1	All electronic signatures applied by electronic delivery services to ERD messages and ERDS evidences shall be UAE advanced electronic signature or advanced electronic seals.

12.4 Provisions related to the inclusion of the related qualified trust service in the UAE trusted list

TL-1	A QTS consisting in the provisioning of electronic delivery service shall be identified in the UAE trusted list in compliance to clause 7.2 of [ETSI EN 522-4-3].

13 Requirements on advanced electronic signatures and advanced electronic seals

13.1 General requirements

GPR-1	Advanced electronic signatures and advanced electronic seals shall be created in accordance with one or more of the following standardized formats: - CAdES format: [ETSI EN 319 122-1], from the CAdES-B-B level; - XAdES format: [ETSI EN 319 132-1], from the XAdES-B-B level; - PAdES format: [ETSI EN 319 142-1], from the PAdES-B-B level; - JAdES format: [ETSI TS 119 182-1], from the JAdES-B-B level; - Signature container format - ASiC: [ETSI EN 319 162-1], from the corresponding B-B level.

13.2 Cryptographic requirements

CRY-1	The cryptographic suites and the cryptographic key lengths and parameters used for the creation of advanced electronic signatures and advanced electronic seals shall be capable to resist to cryptographic attacks during the validity period of the data to which they are applied and, when applicable, of the associated certificate, whichever is the longer.
CRY-2	The cryptographic suites and the cryptographic key lengths and parameters shall conform to the latest version of the SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms [SOG-IS Crypto WG].