Draft ETSI SR 019 003 V0.0.2 (2021-09)

Electronic Signatures and Infrastructures (ESI); Possible Standards for eIDAS 2.0

Send comments ONLY to E-SIGNATURES_COMMENTS@list.etsi.org

Download the template for comments:

https://docbox.etsi.org/ESI/Open/Latest_Drafts/ Template-for-comments -SR 019 003.doc

Reference
SR/ESI-019003

Keywords
e-commerce, electronic signature, electronic identity, security, trust services

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Special Report (SR) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures TC ESI

Executive summary & Introduction

The EU commission have published proposal for amending Regulation (EU) No 910/2014 [1] as regards establishing a framework for a European Digital Identity SEC(2021) 228 final [2], referred to in the present document as eIDAS 2.0. The present document considers the new and amended requirements in eIDAS 2.0 and how existing, planned or new ETSI standards may be used to address these requirements.

Over the past 20 years ETSI TC ESI has published about 70 technical specifications and European norms in support of EU regulatory, as well as global, requirements in the areas relating to electronic signatures and trust services (see: https://portal.etsi.org/TB-SiteMap/esi/esi-activities). This covers requirements for the Electronic Signatures Directive 1999/93/EC, as well as the requirements the requirements of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market.

Existing ETSI eIDAS standards already cover most aspects of the standardisation requirements of eIDAS 2.0. The present document identifies 40 requirements in eIDAS 2.0 which can be met by existing standards, and about 10 other standards which may require updating to fully meet the requirements of eIDAS.

ETSI TC ESI recognises the need for further standards supporting the requirements of Attribute Attestations, such as in Annex V of eIDAS 2.0, and the security of trust services issuing attestations. The security requirements for the issuing of attribute attestation can use the existing general practices for the security of trust services, in EN 319 401, as well adapt existing standards for issuing of certificates in EN 319 411 parts 1 and 2. These standards could also be adopted as the basis of national schemes issuing electronic identification means.

ETSI TC ESI also recognise the need to support the definition of the interfaces between the EU Digital Wallet and trust and digital signature services which are commonly based on existing ETSI standards

ETSI TC ESI has identified standardisation in the following areas as high priority work items:

- Profiles for Attribute Attestation
- Policy and security requirements for Attribute Attestation Services,
- EU Digital ID Wallet interfaces for trust services and signing.

ETSI TC ESI also considers that it's significant experience, working with CEN, in supporting requirements of certification of services based on signing devices as in CEN EN 419 211 parts 1 to 6 and CEN EN 419 241 part 1 and 2, could significantly help in making the EU Digital Wallet a success.

ETSI TC ESI is keen to work with the EU Commission and member nations in the definition standards for eIDAS 2.0 and is able to provide expertise based on 20 years of experience in this area.

1 Scope

The present document identifies the potential impact on a framework of standards in relation to the Proposal for a Regulation of the European parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity[i.2].

In the following table the columns have the following meaning:

1. a reference to eIDAS 2.0 article(s) (i.e. the articles of eIDAS as modified by the Commission proposed Regulation)
2. summary of the topic (the purpose is to be a reminder, please refer to the complete text)
3. type of act (mandatory or not) and timeframe, in reference to Commission requirements for common standards
4. initial identification of possible standardisation to meet of the identified article.:
    - use of existing ETSI standards,
    - updates to existing ETSI standards
    - use of other openly available specifications which may be profiled to meet the EU requirements
    - new ETSI standards

   with an indication of possible need for liaison to coordinate standards development with other organisations.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Regulation (EU) No 910/2014 of the European Parliament and of The Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.2] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity.

Note: available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0281

[i.3] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

[i.4] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (NIS2 Directive)

Note: available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN

[i.5] ETSI TR 119 000 Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview

Other documents are referenced as identified below. The framework for existing ETSI documents supporting eIDAS are identified in the framework document ETSI TR 119 000. ETSI standards can be downloaded at:
https://www.etsi.org/standards

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in Regulation (EU) No 910/2014 [i.1], eIDAS 2.0 (SEC(2021) 228 final) [i.2] and TR 119 001 apply.

3.2 Abbreviations

CEN European Committee for Standardisation

CEF Connecting Europe Facility

EA European co-operation for Accreditation

EBSI European Blockchain Services Infrastructure

NOTE: see https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI

eIDAS Regulation (EU) No 910/2014 [i.1]

eIDAS 2.0 Regulation (EU) No 910/2014 [i.1] as modified by the amending proposal [i.2].

IAF International Accreditation Forum

ISO International Standards Organization

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

NIS2 Proposal for amended Directive on measures for a high common level of cybersecurity [i.4]

TC Technical Committee

UPU Universal Postal Union

W3C World Wide Web Consortium

4 eIDAS 2.0 and Possible Standards

eIDAS 2.0 article	Topic	EC Acts: Should/ Shall	Possible standards – for specific requirement
3	New/updated definitions	-	**updates to existing ETSI standards** *eIDAS 2.0 general: Updates to take into account new standardisation requirements.* TR 119 000 The framework for standardization of signatures: overview *Article 3. new definitions* TR 119 001 The framework for standardization of signatures; Definitions and abbreviations

6a(3), 6a(4) and 6a(5)	European Digital Identity Wallets • securely request, obtain, store, select, combine, share legal person identification data and attestation to authenticate online and offline • sign by means of qualified electronic signatures • provide a common interface to (Q)TSP, relying parties and users • ensure QTSP cannot receive information about the Wallet use • meet assurance level "high" • relying party able to authenticate the user receive electronic attestations • person identification data uniquely and persistently represent the natural or legal person • Member States provide Wallets validation mechanisms	Shall, 6 months, establish technical and operational specifications and reference standards	**use of existing ETSI standards** *Article 6a(3), point (b), sign by means of qualified electronic signatures* TS 119 432 - Protocols for remote digital signature creation **use of other openly available specifications** *Article 6a(4), point (a) (2), for relying parties to request and validate person identification data and electronic attestations of attributes* *& Article 6a(4), point (d): provide a mechanism to ensure that the relying party is able to authenticate the user and to receive electronic attestations of attributes;* OpenID Connect 1.0 specifications for authentication https://openid.net/connect/ *Article 6a: General requirements for European DigitalIdentity Wallets:* ISO FDIS 18013-5 ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application **new ETSI standards** *Article 6a(3), points (a) and (b), and article 4a(1) and (2) .* New ETSI standard on Wallet interfaces for trust services and signing - ETSI High priority See DTS/ESI-0019462 on work programme page: https://portal.etsi.org//tb.aspx?tbid=607&SubTB=607#/ See also new standards for attestation of attributes under Article 45c below.

eIDAS 2.0 article	Topic	EC Acts: Should/ Shall	Possible standards – for specific requirement
			Liaisons CEN/CLC (specific committees to be identified) W3C Credentials Community Group (active) – DID W3C Verifiable Credentials Working Group (in maintenance mode) – Verifiable Credentials FIDO ISO/IEC JTC 1/SC 17 CEN TC 224 EBSI
6b(2)	European Digital Identity Wallets Relying Parties: Member States to implement a common mechanism for the authentication of relying parties	Shall, 6 months, establish technical and operational specifications and reference standards	**use of existing ETSI standards,** EN 319 412-3 – Qualified Certificate for electronic seals for authentication of relying parties EN 319 1x2-1 – AdES signatures for authentication of relying parties EN 319 412-4 – Qualified Website Certificate for authentication of relying parties **use of other openly available specifications** Transport Layer Security RFC 8446 – protocol for authentication of relying parties

eIDAS 2.0 article	Topic	EC Acts: Should/ Shall	Possible standards – for specific requirement
6c	Certification of the European Digital Identity Wallets: Wallets conformity with cybersecurity requirements in article 6a(3), 6a(4) and 6a(5) shall be certified by CABs designated by Member States or CSA scheme. Commission to adopt implementing act with standards for certification and delegated acts on specific criteria to be met by the CABs. Personal data processing compliance shall be certified certification according to GDPR	Shall, 6 months, list of standards	**ETSI Standardisation Coordination** *The existing standard for certification of the security of trust services (EN 319 403-1) could be adapted to apply to services for EU Digital Identities* *ETSI TC Cyber and ETSI TC ESI will work together in order to avoid technical duplications and incompatibilities between NIS2 Directive and eIDAS 2.0 Regulation.* *It should be also looked into the technical impact of the Digitals Services and Digital Markets Acts… in particular with respect to QWACs and the security of the crypto-tokens used for presenting eIDs, credentials and attributes* **Liaisons** CEN/CLC/JTC 13 in particular WG5 on privacy and WG3 on common criteria
6a(4) point (c) 12a(1)	Meet requirements for "high" in particular as applied to the requirements for identity proofing and verification, and electronic identification means management and authentication. Conformity of notified electronic identification schemes with the requirements laid down in Article 6a, Article 8 and Article 10 may be certified by public or **private bodies** designated by Member States.		**updates to existing ETSI standards** *Updated to support "high" identity proofing and verification* TS 119 461 - Policy and security requirements for trust service components providing identity proofing of trust service subjects *New part to support conformity assessment of identity proofing and verification* EN 319 403-x Trust Service Provider Conformity Assessment – conformity assessment of identity proofing and verification

eIDAS 2.0 article	Topic	EC Acts: Should/ Shall	Possible standards – for specific requirement
14	International aspects – Legal equivalence of qualified TSPs	May "conditions under which the requirements of a third country applicable"	**use of existing ETSI standards** *Technical considerations under which trust services in third countries may be considered a equivalent to qualified trust services provided by qualified trust service providers established in the Union* TR 103 684 –report on Global Acceptance of EU Trust Services (In particular, clause 4.2 on areas of comparison) **updates to existing ETSI standards** *Update of existing ETSI standards, or new generalised equivalent standards, to facilitate implementation by third party countries:* TS 119 612 trusted lists TS 119 615 Trusted lists; Procedures for using and interpreting European Union Member States national trusted lists Possible updates to 4x1and 5x1 series documents to provide guidance for international equivalents to EU specific requirements. Possible updates to EN 319 412-5 for declaration of international equivalents to QSCD (esi4-qcStatement-4) **Liaisons** CEF Project on cross recognition on signatures EA & IAF – on international recognition of EN 319 403

20	Qualified Trust Services: accreditation of the CABs and for the conformity assessment report (Art. 20(1))	Shall, 12 months, reference standards	**use of existing ETSI standards** EN 319 403-1 Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers TS 119 403-3 – Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers. *Hopefully legislation will better define the relation between the European eIDAS Conformity assessment scheme and the 27 different national NIS2 Conformity assessment schemes, avoiding duplications and capitalizing on the existing pan-European eIDAS Conformity assessment scheme, that has been established for avoiding that (prima facie) cybersecurity issues become an insurmountable obstacle to a European single market for Qualified Trust Services. Without such clear definition, it will not be easy to technically co-ordinate eIDAS and NIS2 standards and accreditation schemes, with a negative impact on several technical aspects. Relevant coordination issues include:* *a) Coordination between NIS2 and eIDAS 2.0 security requirements. Conflicts can easily be avoided, because the structure of both security policies are similar and share the same roots (ISO 27000)* *b) Coordination between eIDAS Part II national eIDS and eIDAS Part III European eIDS, subjected (also) to a national conformity assessment scheme* *c) Technical definition and technical coordination between Identification Services as defined in art. 2.1.(15) of COM 2020/842 and eIDAS 2.0 eIDs (art. 6a(3), 6a(4),6a(5), etc.).* *d) Technical definition and coordination between Core Platform Services as defined in artt. 1 and 2 of COM 2020/842, and eIDAS QTSs*

eIDAS 2.0 article	Topic	EC Acts: Should/ Shall	Possible standards – for specific requirement
			e) Use of a common International basis for conformity assessment which is aimed specifically at certification of products, processes and services: ISO 17065.
24(1)	technical specifications for verification of identity and attributes of natural persons with a high level of confidence confirmed by a CAB	Shall, 12 months, minimum technical specifications, standards and procedures	**use of existing ETSI standards,** TS 119 461 Policy and security requirements for trust service components providing identity proofing of trust service subjects *May require updates to take into account Attestation of attributes.*

eIDAS 2.0 article	Topic	EC Acts: Should/ Shall	Possible standards – for specific requirement
24(2)	Requirements for qualified trust service providers	Shall, 12 months, reference standards	**use of existing ETSI standards,** EN 319 411-1 & 2: Policy and security requirements for Trust Service Providers issuing certificates; Part1: General requirements Part 2: Requirements for trust service providers issuing EU qualified certificates TS 119 431-1: Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev TS 119 511: Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques EN 319 521: Policy and security requirements for Electronic Registered Delivery Service Providers EN 319 531: Policy and security requirements for Registered Electronic Mail Service Providers **updates to existing ETSI standards** *Possible updates to general requirements of TSP o take into account NSI2, eAccessibility, GDPR, ePrivacy regulations* EN 319 401: General Policy Requirements for Trust Service Providers

eIDAS 2.0 article	Topic	EC Acts: Should/ Shall	Possible standards – for specific requirement
27	Electronic signatures in public services	Member states shall: AdES formats	**use of existing ETSI standards,** *Suggest update to CID 2015/1506 to use current AdES baseline formats standards:* EN 319 122-1: CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures EN 319 132-1: XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures EN 319 142-1: PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures EN 319 162-1: Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers TS 119 182-1: JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures *Note:* TS 119 182-1 m*ay be later replaced by European Norm EN 319 182-1* **new ETSI standards** Possible new AdES format based on CBOR Object Signing and Encryption (COSE)IETF RFC 8152. **Liaisons** W3C, IETF

eIDAS 2.0 article	Topic	EC Acts: Should/ Shall	Possible standards – for specific requirement
28 38	Qualified certificates for electronic signatures + Annex I Qualified certificates for electronic seals + Annex III	Shall, 12 months, reference standards	**use of existing ETSI standards,** EN 319 412-1:Certificate Profiles; Part 1: Overview and common data structures EN 319 412-2: Certificate profiles for natural persons *(For creating electronic signatures / seals)* EN 319 412-3: Certificate profiles for legal persons *(For creating electronic signatures / seals)* EN 319 412-5: Certificate Profiles; Part 5: QCStatements *(General requirements for qualified certificates)*
29a 39a	new articles with requirements for qualified trust service provider for the management of a remote QSigCD (and mutatis mutandis for QSealCD – Art 39a)	Shall, 12 months, technical specifications + reference of standards	**use of existing ETSI standards,** TS 119 431-1: Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev **use of other openly available specifications** CEN EN 419 241-1: Trustworthy Systems Supporting Server Signing Part 1: General System Security Requirements CEN EN 419 241-2: Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing CEN 419 221-5: Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services **Liaisons** CEN TC 224

eIDAS 2.0 article	Topic	EC Acts: Should/ Shall	Possible standards – for specific requirement
30, 39	Certification of qualified electronic signature creation devices New: vulnerability assessment every 2 years, 5 years certification validity	shall (already in force, no deadline), reference standards	**updates to existing ETSI standards** *Possible update to TSP policy requirements to check QSCD status* EN 319 411-2: Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
32	Requirements for the validation of qualified electronic signatures	shall, 12 months, reference standards	**use of existing ETSI standards,** EN 319 102-1: Procedures for Creation and Validation of AdES Digital Signatures [electronic signature or seal] TS 119 172-4: Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists TS 119 615: Trusted lists; Procedures for using and interpreting European Union Member States national trusted lists
33	Qualified validation service for qualified electronic signatures	may	**use of existing ETSI standards,** TS 119 441 Policy requirements for TSP providing signature validation services TS 119 102-2:Validation report

eIDAS 2.0 article	Topic	EC Acts: Should/ Shall	Possible standards – for specific requirement
34	Qualified preservation service for qualified electronic signatures	shall, 12 months, reference standards	**use of existing ETSI standards,** TS 119 511: Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques TS 119 512: Protocols for trust service providers providing long-term data preservation services
37 40	Electronic seals in public services Now requires publication of standards for advanced electronic seals in addition to standards for formats/methods already referenced with CID 2015/1506	shall, 12 months, reference standards + issued CID 2015/1506	*See standards against Article 27 on formats for advanced electronic signatures also applicable to electronic seals.*
42	Requirements for qualified electronic time stamps	shall 12 months	**use of existing ETSI standards,** EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps EN 319 422: Time-stamping protocol and time-stamp token profiles

eIDAS 2.0 article	Topic	EC Acts: Should/ Shall	Possible standards – for specific requirement
44	Requirements for qualified electronic registered delivery services 1a. Compliance with the requirements laid down in paragraph 1 shall be presumed where the process for sending and receiving data meets the standards referred to in paragraph 2	shall, 12 months, reference standards	**use of existing ETSI standards,** EN 319 521: Policy and security requirements for Electronic Registered Delivery Service Providers EN 319 522: Electronic Registered Delivery Services EN 319 531: Policy and security requirements for Registered Electronic Mail Service Providers EN 319 532: Registered Electronic Mail (REM) Services **Liaisons** CEN/TC 331 UPU
45	Requirements for qualified certificates for website authentication – Annex IV shall be recognised by web-browsers that shall ensure that the identity data provided using any of the methods is displayed in a user friendly manner; SME providing browser services excluded for 5 years	shall, 12 months, reference standards	**use of existing ETSI standards,** EN 319 412-4 Certificate Profiles; Part 4: Certificate profile for web site certificates (update under EN approval process) EN 319 412-5 Certificate Profiles; Part 5: QCStatements

45c Annex V	Requirements for qualified attestation of attributes	shall, 6 months, reference to standard	**new ETSI standards** New pair of ETSI standards on Attestation of Attributes covering: - Policy and security requirements for attribute attestation services - Profiles for attribute attestations taking into account Annex V. *High ETSI priority* See DTS/ESI-0019451 and DTS/ESI-0019452 on work programme page: https://portal.etsi.org//tb.aspx?tbid=607&SubTB=607#/ **use of other openly available specifications** The following existing standards have been identified as possible basis of Attestation of Attributes. It is proposed to identify the general sematic requirements for the Attestation of Attributes and profile one or more of the following against the general semantic requirements. • X.509 The Directory: Public-key and attribute certificate frameworks • IETF RFC 5755 An Internet Attribute Certificate Profile for Authorization • W3C Verifiable Credentials Data Model • OASIS SAML • JSON Web Tokens **Liaisons** FIDO, W3C, OASIS, DIF, EBSI, CEN/CLC/JTC19

eIDAS 2.0 article	Topic	EC Acts: Should/ Shall	Possible standards – for specific requirement
45d	Verification of attributes against authentic sources Catalogue of attributes, verification procedures; link with Wallets	shall, 6 months, technical specs from EC, taking into account standards	*See standards against Article 45c on Attestation of Attributes*

45g	Qualified electronic archiving services trust service provider that uses procedures and technologies capable of extending the trustworthiness of the electronic document beyond the technological validity period	Shall, 12 months	**use of existing ETSI standards,** SR 019 510: Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures **updates to existing ETSI standards** *Updates title, scope and possible requirements to specify application to archival services. Also to take into account other standards on archiving – see below.* TS 119 511: Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques TS 119 512: Protocols for trust service providers providing long-term data preservation services **use of other openly available specifications** ISO 11506: Archiving of electronic data — Computer output microform (COM)/Computer output laser disc (COLD) ISO/TR 17797: Electronic archiving — Selection of digital storage media for long term preservation ISO 18565: Document management — AFP/Archive ISO 19005-1: Electronic document file format for long-term preservation — Part 1: Use of PDF 1.4 (PDF/A-1) ISO 19005-2: Electronic document file format for long-term preservation — Part 2: Use of ISO 32000-1 (PDF/A-2) ISO 19005-3: Electronic document file format for long-term preservation — Part 3: Use of ISO 32000-1 with support for embedded files (PDF/A-3)

eIDAS 2.0 article	Topic	EC Acts: Should/ Shall	Possible standards – for specific requirement
			ISO/TC 46/SC 11 Standards on Archives/records management ISO 14721:2012 Space data and information transfer systems, Open archival information system (OAIS), Reference model - ISO 13527:2010 Space data and information transfer systems, XML formatted data unit (XFDU) structure and construction rules **Liaisons** ISO/TC 171 ISO/TC 46 CEN/TC 468

45i	Requirements for qualified electronic ledgers:
	
	One or more QTSP; uniqueness, authenticity, correct sequencing, chronological ordering, accuracy of date/time of data in the ledger; any subsequent change is detectable.
		may, reference to standard	**Use of other openly available specifications**
			
			Number of standards under development in:
			
			- ISO/TC 307
			  ○ ISO 22739:2020 Blockchain and distributed ledger technologies — Vocabulary (also to be adopted as a European Standard by CEN/CLC/JTC 19)
			  ○ ISO/TR 23244:2020 Blockchain and distributed edger technologies — Privacy and personally identifiable information protection considerations
			  See: https://www.iso.org/committee/6266604/x/catalogue/ for list of current work items.
			- IEEE: See: https://blockchain.ieee.org/ and https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/blockchain.pdf
			- ITU-T
			  ○ ITU-T Focus Group on Application of Distributed Ledger Technology: https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx
			  ○ standardization work ongoing in ITU-T Study Groups 16 (Multimedia) and 17 (Security)
			• W3C
			  ○ Decentralized Identifier Working Group (DID WG) https://www.w3.org/2019/did-wg/
			  ○ "Credential Community Group" (https://www.w3.org/community/credentials/) wh ich has developed key standards for SSI (Self-Sovereign Identity)
			• OASIS
			  ○ The Ethereum OASIS Open Project https://github.com/ethereum-oasis/oasis-open-project
			  ○ The Baseline Protocol OASIS Open Project https://www.baseline-protocol.org/

			• UNECE
			  ○ White Papers on Blockchain and a Sectoral Use Case paper:
			  ▪ https://www.unece.org/fileadmin/DAM/cefact/GuidanceMaterials/WhitePaperBlockchain.pdf
			  ▪ https://www.unece.org/fileadmin/DAM/cefact/GuidanceMaterials/WhitePaperBlockchain_TechApplication.pdf
			  ▪ https://www.unece.org/fileadmin/DAM/cefact/cf_plenary/2019_plenary/CEFACT_2019_INF03.pdf
			  ○ work on interoperability of ledgers: https://uncefact.unece.org/display/uncefactpublic/Cross+border+Inter-ledger+exchange+for+Preferential+CoO+using+Blockchain
			
			new ETSI standards
			
			Standards to be developed based on work result on
			SR 019 002: Application of Distributed Ledger Technology to Signatures and Trust Services
			
			Standards applying standards being developed by ETSI ISG on Permissioned Distributed Ledger (PDL) See:
			https://www.etsi.org/committee/1467-pdl
			To eIDAS trust service framework
			
			Liaisons
			CEN/CLC/JTC 19
			
			CEF European Blockchain Services Infrastructure
			
			ISO/TC 307

eIDAS 2.0 article	Topic	EC Acts: Should/ Shall	Possible standards – for specific requirement
			ETSI Industry Specification Group (ISG) Permissioned Distributed Ledger (PDL).
51 (2)	QC issued under Directive 1999/93/EC to lose qualified status from enter into force + 4 years		**updates to existing ETSI standards** Impact on ETSI standards to be evaluated.

History

Document history		
September 2021	V0.0.2	Draft for public review