ETSI TS 119 541 V1.1.1 (2025-10)

TECHNICAL SPECIFICATION

Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Smart Contracts using Electronic Ledgers

Reference
DTS/ESI-0019541

Keywords
digital identity, digital signature, smart contract,
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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights 5
Foreword 5
Modal verbs terminology 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 7
3 Definition of terms, symbols, abbreviations and notations 8
3.1 Terms 8
3.2 Symbols 8
3.3 Abbreviations 8
3.4 Notations 8
4 Policy framework introduction 9
5 Risk Assessment 10
6 SC provider Policies and practices 10
6.1 SC provider Service Practice statement 10
6.2 Terms and Conditions 11
6.3 Information security policy 12
7 SC provider management and operation 13
7.1 Internal organization 13
7.1.1 General 13
7.1.2 Organization reliability 13
7.1.3 Segregation of duties 13
7.2 Human resources 13
7.3 Asset management 13
7.3.1 General requirements 13
7.3.2 Assets inventory and classification 13
7.3.3 Storage media handling 13
7.4 Access control 14
7.5 Cryptographic controls 14
7.6 Physical and environmental security 14
7.7 Operation security 14
7.8 Network security 14
7.9 Vulnerabilities and Incident management 14
7.9.1 Monitoring and logging 14
7.9.2 Incident response 14
7.9.3 Reporting 14
7.9.4 Event assessment and classification 14
7.9.5 Post-incident reviews 15
7.10 Collection of evidence 15
7.11 Business continuity management 15
7.11.1 General 15
7.11.2 Back up 15
7.11.3 Crisis management 15
7.12 Termination and termination plans 15
7.13 Compliance 15
8 SC Provider and SC Supply Chain Requirements 15
8.1 General 15
8.2 SC Publisher 15
8.3 SC Language Publisher and Supporting Tools Publishers 16
8.4 SC Provider 16
8.5 Electronic Ledger Provider(s) 16

Annex A (normative): Security framework and requirements 18
A.1 Security analysis and justifications 18
A.2 Requirements for Confidentiality, Integrity and Availability (CIA) 18
A.2.1 Confidentiality requirements 18
A.2.2 Integrity requirement 19
A.2.3 Availability requirements 19
A.3 Non-repudiation requirements 19
A.4 GDPR risk and obligations 19
Annex B (informative): Audit requirements 21
Annex C (informative): CRA essential requirements and impact on SC 22
C.1 Essential requirements identified in Annex I of the CRA 22
C.2 Requirements for vulnerability handling identified in Annex I of the CRA 23
Annex D (informative): Bibliography 25
History 26

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Trust Infrastructures (ESI).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document specifies the policy and security requirements for Smart Contracts using Electronic Ledgers as defined in Regulation (EU) 910/2014 amended by Regulation (EU) 2024/1183 [i.3], and with other trustworthy tools, taking into account the framework of requirements identified in ETSI TR 119 540 [i.1].

NOTE 1: The present document extends provisions from ETSI EN 319 401 [1] and TS 18264 [2], using the structure of ETSI EN 319 401 [1] as the basis, to address the general requirements identified by the Chain of Trust described in clause 5.1 of [i.1].

NOTE 2: When applying ETSI EN 319 401 [1] to the scope and context of the present document any reference in ETSI EN 319 401 [1] to TSP is to be read as "SC Provider".

NOTE 3: In ETSI EN 319 401 [1] there are references to "management bodies" which for the purposes of the present document is to be read as an entity within the SC provider's organization with a defined role identifiable using methods defined in ETSI TS 119 542 [5].

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

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 necessary for the application of the present document.

[1] ETSI EN 319 401: "Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[2] TS 18264: "Policy and security requirements on trust services on electronic ledgers", (produced by CEN/CENELEC).

NOTE 1: The present document extends the above to address the specificities for Smart Contracts.

NOTE 2: Under approval at time of writing.

[3] ETSI EN 319 403-1: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers".

[4] ISO 23257:2022: "Blockchain and distributed ledger technologies — Reference architecture".

[5] ETSI TS 119 542: "Electronic Signatures and Trust Infrastructures (ESI); Use of EU Digital Identity Wallets and electronic signatures for identification with smart contracts".

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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI TR 119 540: "Electronic Signatures and Trust Infrastructures (ESI); Standardisation requirements for smart contracts based on electronic ledgers".

[i.2] ETSI EN 319 411-1: "Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

[i.3] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

[i.4] CA/Browser forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates Version 3.9.0".

[i.5] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).

[i.6] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[i.7] ETSI GS PDL 003: "Permissioned Distributed Ledger (PDL); Smart Contracts; System Architecture and Functional Specification".

NOTE: The above reference applies only where the provisions extend those identified in ISO 23257 [4].

[i.8] ENISA/JRC: "Cyber Resilience Act Requirements Standards Mapping", Joint Research Centre & ENISA Joint Analysis.

[i.9] ETSI Guide to the Use of English for drafting ETSI deliverables.

[i.10] ETSI TR 103 838: "Cyber Security; Guide to Coordinated Vulnerability Disclosure".

[i.11] ETSI EN 303 645: "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".

[i.12] ETSI TR 104 034: "Cyber Security (CYBER); Software Bill of Materials (SBOM) Compendium".

[i.13] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).

[i.14] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[i.15] ISO/IEC 27002:2022: "Information security, cybersecurity and privacy protection — Information security controls".

3 Definition of terms, symbols, abbreviations and notations

3.1 Terms

For the purposes of the present document, the terms given in the Data Act [i.13], ETSI EN 319 401 [1], ETSI TR 119 540 [i.1] and the following apply:

governance: action or manner of governing the Smart Contract and its stakeholders

policy: course or principle of action adopted or proposed by an organization or individual

trustworthy: able to be relied on as honest or truthful

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CA	Certificate Authority
CIA	Confidentiality Integrity Availability
CRA	Cyber Resilience Act
DPIA	Data Privacy Impact Assessment
ENISA	European Network and Information Security Agency
GDPR	General Data Protection Regulation
NIS2	Network and Information Security (directive version 2)
SBOM	Software Bill of Materials
SC	Smart Contract
T&C	Terms and Conditions
TSP	Trust Service Providers
URL	Uniform Resource Locator
VM	Virtual Machine

3.4 Notations

The requirements in the present document are identified as follows:

- <the 3 letters REQ> - < the clause number> - <2 digit number - incremental> <change indicator / previous addition>

The management of the requirement identifiers throughout subsequent editions of the present document is as follows:

- When a requirement is inserted at the end of a clause, the 2 digit number above is incremented to the next available digit.

4 Policy framework introduction

The present document extends the general overview of the Smart Contract system described in ETSI TR 119 540 [i.1]. In particular the present document specifies the policy and security requirements for Smart Contracts using Electronic Ledgers as defined by the Chain of Trust described in clause 5.1 of ETSI TR 119 540 [i.1], that applies over the lifecycle outlined below and which is described in detail in ETSI TR 119 540 [i.1]:

- SC Provision
  - Involves all entities responsible for delivering the Smart Contract as executable code
- SC Deployment
  - Ensures the secure storage of transaction data in an Electronic Ledger
- SC Execution
  - Ensures that state transitions of the contract are agreed and recorded

The Smart Contract Provider is responsible for the provision of a Smart Contract (SC) to users. The SC executes a computer program as published by a SC computer program publisher. The computer program is written in a language published by a responsible entity and the language that is published includes supporting tools such a compiler and language specification which are used by the SC Program Publisher's development team. The SC provider can also utilize a byte code interpreter / virtual machine provided by the language publisher.

The SC provider shall be determined by the responsibility it holds towards the users of the Smart Contract.

The SC provider shall be responsible for making sure the Smart Contract works correctly and reliably.

The SC Provider uses an Electronic Ledger to record transaction data which contributes to the contract being formed. This transaction data can later be retrieved by the same or another SC Provider to further build on the contract. The Electronic Ledger can also be used to distribute a SC Program.

NOTE 1: In the context of SCs the Ledger records things, the SC provider executes things (that may be recorded on the ledger).

Each of the above providers / publishers has a policy which defines the specific security and functional techniques applied by the organization. The present document defines the Core Policy requirements for the SC Provider (see clauses 7 (SC provider management and operation) and 8 (SC Provider and SC Supply Chain Requirements)). This Core Policy places requirements on the Smart Contract Program Publisher (including its development team) to meet separate policy requirements on the Smart Contract Program development and maintenance (see clause 8.2). The Core Policy and the Smart Contract Program Policy also place requirements on the Smart Contract Language Publisher (including its development and maintenance team) to meet separate policy requirements on the Smart Contract Language development and maintenance (see clause 8.3).

The present document does not specify policy and security requirements on the Electronic Ledger provider. The Electronic Ledger can be Qualified or Non-Qualified. The Electronic Ledger can consist of a single TSP or provided by a community of TSPs supporting aligned policies.

NOTE 2: A standard for Policy and Security Requirements for Trust Service Providers Providing Electronic Ledger Services is under approval in CEN/CLC/JTC19 at the time of writing (see TS 18264 [2]).

The Smart Contract Provider and a TSP providing all or part of an Electronic Ledger can be the same legal entity. Thus, whilst provision of Smart Contract services is not a trust service as specified in as specified in Regulation 2024/1183 [i.3] amending Regulation 910/2014, the present document applies the same general security and policy requirements for trust service providers as specified in ETSI EN 319 401 [1]. Therefore the policy framework and the resulting document structure for Smart Contract are derived from the general policy requirements on Trust Service Providers (TSPs) specified in ETSI EN 319 401 [1] augmented and informed by ETSI TR 119 540 [i.1], and informed by the security policy framework for TSPs as specified in ETSI EN 319 411-1 [i.2]. In addition the specific technical security requirements from ledger perspective defined in TS 18264 [2] are adopted and highlighted in the succeeding clauses of the present document. Where appropriate the present document adopts the requirements from ETSI EN 319 401 [1], from ETSI GS PDL 003 [i.7], from ISO 23257 [4] and from TS 18264 [2] with any identified restrictions or extensions marked.

If the same legal entity provides the services of a Smart Contract Provider and a TSP providing all or part of an Electronic Ledger, then conformance to the present document and Policy and Security Requirements for Trust Service Providers Providing Electronic Ledger Services can be certified together under ETSI EN 319 403-1 [3].

NOTE 3: A ledger in the form identified in ETSI GS PDL 003 [i.7], ISO 23257 [4] and in TS 18264 [2] is read only once data has been accepted by consensus, and data is then persistent, therefore obligations from GDPR [i.14] need to be clearly addressed (see also clause A.4 of the present document).

EXAMPLE: Where the security policy of the Smart Contract as executable code requires that code signing is adopted in which case the policy requirements identified in the succeeding clauses can be enhanced by adoption of the code signing principles published by the CA/B forum [i.4].

5 Risk Assessment

The provisions of ETSI EN 319 401 [1], clause 5 apply in general with the specific wording changes given below.

REQ-5-01: The SC provider shall carry out a risk assessment to identify, analyse and evaluate risks taking into account business and technical issues in particular addressing the supply chain issues as in clause 8 of the present document.

NOTE 1: In ETSI EN 301 401 [1], clause 5 the risk assessment is made with respect to the Trust Service Provider undertaking the risk assessment actions, whereas for the present document the SC provider is assumed to have maximum liability as the only entity in the trust chain with a relationship to the SC User. That notwithstanding all stakeholders in the supply chain are expected to have carried out a risk assessment with respect to their own role in the provision of Smart Contracts as outlined in ETSI TR 119 540 [i.1].

REQ-5-02: The SC provider shall select the appropriate risk treatment measures, taking account of the risk assessment results. The risk treatment measures shall ensure that the level of security is commensurate to the degree of risk.

NOTE 2: The native mechanisms of Electronic Ledgers, when deployed may be sufficient and appropriate to act as risk treatment measures.

REQ-5-03: The SC provider shall determine all security requirements and operational procedures that are necessary to implement the risk treatment measures chosen, as documented in clauses 6, 7 and 8 of the present document.

REQ-5-04: The risk assessment shall be regularly reviewed and revised.

NOTE 3: One intent of REQ-5-04 is to consider that REQ-5-01 is recursive and that the provision of risk treatment measures as identified in REQ-5-02 and REQ-5-03 is also revised appropriately.

NOTE 4: The requirement text from [1] may be revised.

REQ-5-05: The responsible entity of the SC provider (e.g. a specified SC provider management role) shall approve the risk assessment and accept the residual risk identified.

REQ-5-05a: The responsible entity of the SC provider to approve the risk assessment and accept the residual risk shall be identifiable using methods defined in ETSI TS 119 542 [5].

REQ-5-06: The SC provider shall perform a DPIA as outlined in GDPR [i.14], Article 35 in order to determine the risk to personal data.

6 SC provider Policies and practices

6.1 SC provider Service Practice statement

The provisions of ETSI EN 319 401 [1], clause 6.1 apply in general with the specific wording changes from TSP to entities in the SC Context given below.

REQ-6.1-01: The SC provider shall specify the set of policies and practices appropriate for the SC services it is providing.

REQ-6.1-02: The set of policies and practices shall be approved by a responsible entity of the SC provider (e.g. a specified SC provider management role), published and communicated to employees and external parties as relevant.

NOTE: ETSI EN 319 401 [1] identifies a number of obligations over external organizations that are addressed for the purposes of the present document by the requirements identified in clause 8 that apply to the SC supply chain.

REQ-6.1-02a: The responsible entity of the SC provider to approve the set of policies and practices shall be identifiable using methods defined in ETSI TS 119 542 [5].

6.2 Terms and Conditions

The provisions of ETSI EN 319 401 [1], clause 6.2 apply in general with the specific wording changes from TSP to entities in the SC Context given below.

REQ-6.2-01: The SC provider shall make the terms and conditions regarding its services available to all SC users and relying parties.

REQ-6.2-02: The terms and conditions shall specify, for each service supported by the SC provider, the following:

a) the SC policy being applied;

b) any limitations on the use of the service provided including the limitation for damages arising from the use of services exceeding such limitations;

EXAMPLE 1: The expected life-time of public key certificates.

c) the obligations of each stakeholder, if any;

d) information for parties relying on the service;

e) the period of time during which event logs are retained;

f) limitations of liability;

g) the applicable legal system;

h) procedures for complaints and dispute settlement;

i) whether the service has been assessed to be conformant with the service policy, and if so through which conformity assessment scheme;

j) the SC Provider's contact information; and

k) any undertaking regarding availability.

REQ-6.2-03: Parties relying on the service provided by the SC provider shall be informed of precise terms and conditions, including the items listed above, before entering into a contractual relationship.

REQ-6.2-04: Terms and conditions shall be made available through a durable means of communication.

NOTE: Whilst adopting REQ-6.2-04 from [1] it is made clear that the term "durable means of communication" means that the T&Cs are available by a means that endures, or persists, throughout the validity period of the SC.

EXAMPLE 2: The Terms and Conditions (T&Cs) related to a specific SC service may be available on the website of the SC Provider in which case the URL/URI that links to the T&C page should be a persistent link.

REQ-6.2-05: Terms and conditions shall be available in a readily understandable language.

EXAMPLE 3: A readily understandable language is one that is understandable to all parties to the SC, e.g. in the EU one of the recognized official languages of the EU. In addition guidelines that apply to clarity, brevity, precision should be applied wherever possible (see for example ETSI's guide to the use of English for drafting ETSI deliverables [i.9]).

REQ-6.2-06: Terms and conditions may be transmitted electronically.

REQ-6.2-07: The terms and conditions shall make clear how obligations from GDPR [i.14], in particular Article 16 (Right to rectification), and Article 17 (Right to erasure), are addressed where data is stored on an Electronic Ledger.

REQ-6.2-08: The SC publisher shall ensure and record that the deployment policy meets the requirements for deployment in the SC Legal Text (see ETSI TR 119 540 [i.1]).

6.3 Information security policy

The provisions of ETSI EN 319 401 [1], clause 6.3 apply in general with the specific wording changes from TSP to entities in the SC Context given below.

REQ-6.3-01: The SC provider shall define a policy on the security of network and information systems which is approved by management and which sets out the SC Provider's approach to managing the security of its network and information systems, that:

a) is appropriate to and complementary with the SC provider's business strategy and objectives;

b) sets out network and information security objectives;

c) includes a commitment to continual improvement of the security of network and information systems;

d) includes a commitment to provide the appropriate resources needed for its implementation, including the necessary staff, financial resources, processes, tools and technologies;

e) is communicated to and acknowledged by relevant employees and relevant interested external parties;

f) lays down roles and responsibilities pursuant to clause 7.1;

g) lists the documentation to be kept and the duration of retention of the documentation;

h) lists the topic-specific policies;

i) lays down indicators and measures to monitor its implementation and the current status of the maturity level of network and information security; and

j) indicates the date of the formal approval by the management bodies of the SC Provider.

REQ-6.3-02: Changes to the information security policy shall be communicated to third parties, where applicable. This includes subscribers, relying parties, assessment bodies, supervisory or other regulatory bodies.

In particular:

REQ-6.3-03: The policy on the security of network and information systems shall be:

a) Documented, implemented and maintained including the security controls and operating procedures for the facilities, systems and information assets providing the services.

b) Reviewed and, where appropriate, updated by management bodies at least annually and when significant incidents or significant changes to operations or risks occur. The result of the reviews shall be documented.

REQ-6.3-04: The SC Provider shall establish procedures to notify of important changes in the provision of the trust service to the appropriate parties in accordance with business requirements and relevant laws and regulations, including changes in the provision of trust services and the intention to cease on its provision.

NOTE 1: Trust service providers qualified according to Directive (EU) 2022/2555 [i.6] amending Regulation (EU) 910/2014 are required to inform the supervisory body of any change in the provision of its qualified trust services and an intention to cease those activities.

REQ-6.3-05: The SC Provider shall publish and communicate the information security policy to all employees who are impacted by it.

NOTE 2: See clause 5.1 of ISO/IEC 27002 [i.15] for guidance.

REQ-6.3-06: The SC Provider's policy on the security of network and information systems and inventory of assets for information security (see clause 7.3) shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

REQ-6.3-07: Any changes that will impact on the level of security provided shall be approved by the management body.

NOTE 3: In ETSI EN 319 401 [1] there are references to "management bodies" which for the purposes of the present document is to be read as an entity within the SC provider's organization with a defined role identifiable using methods defined in ETSI TS 119 542 [5].

REQ-6.3-08: The configuration of the systems in the provision of SC shall be regularly checked for changes which violate the SC Provider's security policies.

REQ-6.3-09: The maximum interval between two checks shall be documented in the trust service practice statement.

NOTE 4: Further recommendations are given in the CA/Browser Forum network security guide [i.4], item 1.

7 SC provider management and operation

7.1 Internal organization

7.1.1 General

The provisions of ETSI EN 319 401 [1], clause 7.1 apply.

7.1.2 Organization reliability

The provisions of ETSI EN 319 401 [1], clause 7.1.2 apply.

7.1.3 Segregation of duties

The provisions of ETSI EN 319 401 [1], clause 7.1.3 apply.

7.2 Human resources

The provisions of ETSI EN 319 401 [1], clause 7.2 apply.

7.3 Asset management

7.3.1 General requirements

The provisions of ETSI EN 319 401 [1], clause 7.3.1 apply.

7.3.2 Assets inventory and classification

The provisions of ETSI EN 319 401 [1], clause 7.3.2 apply.

7.3.3 Storage media handling

The provisions of ETSI EN 319 401 [1], clause 7.3.3 apply.

Where an Electronic Ledger is used the provisions of TS 18264 [2] apply.

7.4 Access control

The provisions of ETSI EN 319 401 [1], clause 7.4 apply.

7.5 Cryptographic controls

The provisions of ETSI EN 319 401 [1], clause 7.5 apply with the change of language from TSP to entities in the SC Context.

NOTE: Due consideration should be made for crypto-agility to address any requirements to change algorithms either due to unanticipated advances in cryptanalysis, to changes in authoritative guidance on algorithms or key sizes, or to advances in quantum computing, any of which render the cryptographic operations null or which substantially weaken them.

7.6 Physical and environmental security

The provisions of ETSI EN 319 401 [1], clause 7.6 apply.

7.7 Operation security

The provisions of ETSI EN 319 401 [1], clause 7.7 apply.

7.8 Network security

The provisions of ETSI EN 319 401 [1], clause 7.8 apply.

NOTE: See also the provisions for NIS2 [i.6] and CRA [i.5] (see Annex C of the present document for a listing of the essential requirements of the CRA).

7.9 Vulnerabilities and Incident management

7.9.1 Monitoring and logging

The provisions of ETSI EN 319 401 [1], clause 7.9.1 apply with the following notes applied to ensure wider compliance with NIS2 [i.6] and CRA [i.5].

NOTE 1: In ETSI additional work is being coordinated to address a common vulnerability reporting capability that corresponds to requirements identified in each of NIS2 [i.6], and CRA [i.5] and should be applied where applicable and as determined by any citation under any of the identified regulations.

NOTE 2: See clause C.2 of the present document for a listing of the essential requirements relating to vulnerability handling of the CRA [i.5].

7.9.2 Incident response

The provisions of ETSI EN 319 401 [1], clause 7.9.2 apply with the suggested extensions of clause C.2 for CRA [i.5].

7.9.3 Reporting

The provisions of ETSI EN 319 401 [1], clause 7.9.3 apply.

7.9.4 Event assessment and classification

The provisions of ETSI EN 319 401 [1], clause 7.9.4 apply.

7.9.5 Post-incident reviews

The provisions of ETSI EN 319 401 [1], clause 7.9.5 apply.

7.10 Collection of evidence

The provisions of ETSI EN 319 401 [1], clause 7.10 apply.

7.11 Business continuity management

7.11.1 General

The provisions of ETSI EN 319 401 [1], clause 7.11.1 apply.

7.11.2 Back up

The provisions of ETSI EN 319 401 [1], clause 7.11.2 apply.

7.11.3 Crisis management

The provisions of ETSI EN 319 401 [1], clause 7.11.3 apply.

7.12 Termination and termination plans

The provisions of ETSI EN 319 401 [1], clause 7.12 apply.

7.13 Compliance

The provisions of ETSI EN 319 401 [1], clause 7.13 apply.

See also the audit requirements outlined in Annex B.

8 SC Provider and SC Supply Chain Requirements

8.1 General

The provisions of ETSI EN 319 401 [1], clause 7.14 apply.

8.2 SC Publisher

REQ-8.2-1: The provisions given in clause 5 of the present document apply to the SC publisher.

NOTE: Where the publisher provides T&Cs or other texts that place obligations on any party there should be proof that those obligations are met.

REQ-8.2-2: The SC Publisher shall specify the set of policies and practices for the development of the SC.

REQ-8.2-3: The SC Publisher shall ensure that the of policies and practices for the development of the SC are applied by the SC Development Team.

REQ-8.2-4: The SC Publisher shall ensure that SC meets the requirements of GDPR [i.14], including any use of Electronic Ledgers.

REQ-8.2-5: SC policies and practices shall ensure that the employed SC Compiler and SC VM come from a SC Compiler that is recognized as conforming to the SC Language.

8.3 SC Language Publisher and Supporting Tools Publishers

REQ-8.3-1: The SC Language Publisher shall specify the language with well defined semantics and syntax.

REQ-8.3.2: The publisher of any SC Language software tool (e.g. compiler, virtual machine interpreting compiler byte code) shall ensure that it conforms to the SC Language from an identified publisher responsible for the SC Language.

8.4 SC Provider

REQ-8.4-1: The SC Provider shall ensure that the Smart Contract has been designed to offer access control mechanisms and a very high degree of robustness to avoid functional errors and to withstand manipulation by third parties.

NOTE: The nature of a Smart Contract on a digital ledger is able to control many of the access control and robustness requirements natively by appropriate selection of the architecture and of the consensus mechanism.

REQ-8.4-2: The SC Provider shall ensure that a mechanism exists to terminate the continued execution of transactions and that the Smart Contract includes internal functions which can reset or instruct the contract to stop or interrupt the operation, in particular to avoid future accidental executions.

REQ-8.4-3: The SC Provider shall ensure, in circumstances in which a Smart Contract has to be terminated or deactivated, there is a possibility to archive the transactional data, the Smart Contract logic and code in order to keep the record of the operations performed on the data in the past (auditability).

REQ-8.4-4: The SC Provider shall ensure consistency with the terms of the data sharing agreement that the Smart Contract executes. The consistency requirement shall be assured by ensuring that the data sharing agreement in natural language can be mapped to the byte-code and virtual machine environment.

8.5 Electronic Ledger Provider(s)

REQ-8.5-1: Electronic Ledger Provider(s) shall apply the requirements of ETSI EN 319 401 [1] as appropriate to the services that they provide.

REQ-8.5-2: The Electronic Ledger Provider(s) shall protect records to meet the objectives defined in Regulation 910/2014, as revised by Regulation (EU) 2024/1183 [i.3], Article 3.

NOTE 1: Regulation (EU) 2024/1183 [i.3], Article 3 (52) states "electronic ledger" means a sequence of electronic data records, ensuring the integrity of those records and the accuracy of the chronological ordering of those records.

REQ-8.5-3: Electronic Ledger Provider(s) shall be independently assessed against a common policy.

NOTE 2: A Technical Specification is under development in CEN/CLC JTC19 for Policy and Security Requirements on Trust Services on Electronic Ledger [2] which may be used as the basis for a common policy for Electronic Ledger Providers.

REQ-8.5-4: The security practices recommended in TS 18264 [2] shall apply.

REQ-8.5-5: Electronic Ledgers in the context of Smart Contracts shall meet the requirements specified in TS 18264 [2] and the following:

a) they are created and managed by one or more providers;

b) they establish the origin of data records in the ledger;

c) they ensure the unique sequential chronological ordering of data records in the ledger;

d) they record data in such a way that any subsequent change to the data is immediately detectable, ensuring their integrity over time.

Annex A (normative): Security framework and requirements

A.1 Security analysis and justifications

A simplified risk analysis is presented in ETSI TR 119 540 [i.1] and expanded in the present document to define in detail the security requirements.

A Smart Contract is defined by the Data Act [i.13] as "*a computer program used for the automated execution of an agreement or part thereof, using a sequence of electronic data records and ensuring their integrity and the accuracy of their chronological ordering*". As identified in ETSI EN 319 401 [1] the following objectives can be derived directly from the definition and the wider application of that definition to that of a contract (an agreement that is intended to be enforceable by law) and to the execution of a contract (the process of finalizing a legally binding contractual agreement between two or more parties and committing to the terms contained within that contract):

1) The automated execution of an agreement, or part thereof, represents the intended agreement of the parties.

2) The parties of the agreement can be correctly identified in case of legal dispute.

3) The recording of the sequence electronic records representing the agreement is maintained in a way which ensures their integrity and the accuracy of their chronological ordering.

4) A party of an agreement cannot later deny the agreement.

5) Privacy of sensitive information is maintained. This can include information in the data records and identities the parties of the agreement.

Within the EU the elements of the Smart Contract shall be bound to the governance frameworks for identity as identified in ETSI TS 119 542 [5] (e.g. eIDAS2 [i.3] to enable strict conformance to objective 2).

In addition it is recognized that contracts as defined in the Data Act [i.13] are, implicitly, required to be transparent and explicable, arising from both objectives 1 and 2 above wherein the parties are able to agree that the Smart Contract, as code (see the definition in clause 3.1 of ETSI TR 119 540 [i.1]), is the intended agreement of the parties. It is noted that the identities of the parties to the agreement are only required to be identified by 3rd parties in the case of legal dispute and in accordance with objective 5 it is reasonable to treat the identity of parties to the agreement as private.

Objective 4 above implies that the SC implements a non-repudiation capability (see clause A.3 for more details).

It is noted that where there are obligations to support some aspects of GDPR such as the right to erasure (Article 17 of GDPR [i.14]) care has to be taken to ensure that the integrity of the ledger is maintained. See clause A.4 for more details.

A conventional risk analysis to determine the risk of an attack identifies the impact of the attack and the likelihood of the attack. In most cases the impact is considered immutable whereas likelihood is considered mutable (i.e. by application of protective countermeasures the likelihood of an attack can be mitigated, ideally to zero, to ensure that risk is minimized).

A.2 Requirements for Confidentiality, Integrity and Availability (CIA)

A.2.1 Confidentiality requirements

A contract is a privileged element, i.e. the parties able to enact the contract are limited, but is not of itself secret and has no specific requirement to be wholly confidential. Parties to the contract may be identified by role or some other attribute, i.e. can be represented pseudonymously.

A Smart Contract implemented in a distributed digital ledger has a number of native confidentiality features that should be enabled as identified by the risk assessment (see clause 5 of the present document).

NOTE: The native mechanisms of distributed ledgers may give assurance of confidentiality.

A.2.2 Integrity requirement

An executable element of the contract shall not be modifiable without evidence of the modification being apparent.

A Smart Contract implemented in a distributed digital ledger has a number of native integrity protection features that should be enabled as identified by the risk assessment (see clause 5 of the present document).

The integrity of each record stored in the ledger shall be assured against unauthorised modification.

NOTE: The native mechanisms of distributed ledgers may give assurance of integrity.

A.2.3 Availability requirements

In the CIA paradigm availability is often expanded to address identification, authentication and access control in order to ensure the protected asset is available to appropriate parties at the time and location that it is needed.

An Electronic Ledger may exist in several formats where the format describes the access control restrictions to the content of the ledger.

NOTE: The native mechanisms of distributed ledgers may give assurance of availability.

A.3 Non-repudiation requirements

As required by objective 4 stated in clause A.1 of the present document parties to the contract shall not be able to deny any action taken on the contract (including observation). Any entry to the Smart Contract, and any event related to the Smart Contract leading to a change of state shall be strongly linked to an identifiable party (i.e. the identified party is authenticated) and securely timestamped. The record of any action shall form part of the immutable digital ledger.

With respect to distributed Electronic Ledgers the general understanding it that once a transaction is recorded on the ledger, it cannot be altered or deleted, ensuring the integrity of the transaction and its place in the record. This immutable record provides strong evidence of the parties' involvement and actions, enabling non-repudiation in digital transactions. In addition each transaction to the record is timestamped and signed by the recording party.

A.4 GDPR risk and obligations

As stated in note 1 of clause 4 in the context of Smart Contracts the Ledger records things, the SC provider executes things (that may be recorded on the ledger). The execution of the SC and the subsequent recording of the results of any execution stage should therefore be guided by the results of a Data Privacy Impact Assessment (DPIA) to determine the degree to which GDPR obligations apply.

The specific actions required are addressed in Article 35 of GDPR [i.14] and shall result in the following items:

- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1 of Article 35 of GDPR [i.14]; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation (i.e. GDPR) taking into account the rights and legitimate interests of data subjects and other persons concerned.

If it is deemed that personal data is collected or processed by the SC the SC Provider shall ensure that it identifies the Data Controller and the Data Processor. Where possible as both these roles are identifiable entities the identification modes identified in ETSI TS 119 542 [5] shall be applied.

In the SC context the Data Controller is mapped to the SC Provider and the Data Processor is mapped to the SC itself. These mappings are taken with respect to the definitions given in Article 3 of [i.14].

The nature of a distributed Electronic Ledger may appear to conflict with specific requirements in GDPR [i.14], in particular Article 16 (Right to rectification), and Article 17 (Right to erasure). Direct conflict with these articles can be avoided if personal data is not stored which may or may not be practical depending on the nature of the contract and how signed data appears in the persistent store. As a digital ledger once written is immutable in order to meet the integrity requirement (see clause A.2.2), and distributed across many storage locations (see clause A.2.3) the remaining mitigations depend on reasonable provisions in the Terms and Conditions offered by the SC Provider (see clause 6.2 of the present document).

Annex B (informative): Audit requirements

Audit requirements are addressed in ETSI EN 319 403-1 [3] with the following notes for interpretation in the SC context, in particular any application of ETSI EN 319 403-1 [3] to the SC environment/context would replace references to the TSP environment/context to equivalent terms and references from the SC environment/context.

In clause 6.2.1.7 of ETSI EN 319 403-1 [3] "Competences for Technical Experts" the list of example competences should be extended to include "knowledge of technologies applicable to the Smart Contract service being audited".

In clause 6.2.1.7 of ETSI EN 319 403-1 [3], as above, the Audit Team should have demonstrable knowledge of the legal, technical and risk factors of Smart Contracts.

Annex C (informative): CRA essential requirements and impact on SC

C.1 Essential requirements identified in Annex I of the CRA

The following essential requirements are identified in the Cyber Resilience Act (CRA) [i.5] and should be taken into consideration when implementing an SC (see also the ENISA report on the CRA standards gap [i.8]). Guidance notes regarding the implementation are identified in Table C.1.

Table C.1: Essential requirements from Annex I of CRA mapped to SC context

Text from CRA			Comment relating to SC application (optional)
1	Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.		This is addressed in clause 5 of the present document.
2	On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:		
	a	be made available on the market without known exploitable vulnerabilities;	
	b	be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;	
	c	ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them;	
	d	ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;	In the context of the present document data records are persistently held on the ledger and once agreed (committed by consensus) cannot be modified. The specifics of the parties agreeing consensus are agreed by the policy elements identified in clause 7.4 of the present document.
	e	protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means;	
	f	protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions;	
	g	process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimization);	
	h	protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;	The use of a persistent ledger whose data is immutable once agreed (committed by consensus) assures resilience of the SC.
	i	minimize the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;	

Text from CRA			Comment relating to SC application (optional)
	j	be designed, developed and produced to limit attack surfaces, including external interfaces;	
	k	be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;	
	l	provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user;	
	m	provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.	Where data is stored on a digital ledger chain it cannot be deleted without destroying the historical integrity of the chain.

C.2 Requirements for vulnerability handling identified in Annex I of the CRA

The following requirements are identified in the Cyber Resilience Act (CRA) [i.5] with regards to handling of vulnerabilities and should be taken into consideration when implementing an SC (see also the ENISA report on the CRA standards gap [i.8]). Guidance notes regarding the implementation are identified in Table C.2.

Table C.2: CRA Vulnerability handling requirements mapping to SC context

Manufacturers of products with digital elements shall:		Comments with respect to SC (optional)
(1)	identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products;	Not specific to SC. The documenting of vulnerabilities should be a component of the technical risk analysis (see clause 5 of the present document). For the role of SBOMs the guidance given in ETSI EN 303 645 [i.11], and in ETSI TR 104 034 [i.12] should be taken into account.
(2)	in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;	Not specific to SC. This is also consistent with the recursive nature of risk assessment addressed in clause 5 of the present document.
(3)	apply effective and regular tests and reviews of the security of the product with digital elements;	Not specific to SC. This is also consistent with the recursive nature of risk assessment addressed in clause 5 of the present document.
(4)	once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;	Not specific to SC. This is being addressed by new activity in CEN in response to the Standardisation Request. In addition ETSI TR 103 838 [i.10] applies. Additionally work in ETSI on the CYBEX protocol/framework applies.
(5)	put in place and enforce a policy on coordinated vulnerability disclosure;	Not specific to SC.
(6)	take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third-party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;	Not specific to SC.
(7)	provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner;	Not specific to SC.
(8)	ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.	Not specific to SC.

Where requirements related to vulnerability reporting are marked as not specific to SC it is to be made clear that the obligations still apply and that such obligations are to be met irrespective of the role of any organization if they provide or enable digital elements.

Annex D (informative): Bibliography

- ETSI EN 319 521: "Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers".
- ETSI TS 119 411-5: "Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 5: Implementation of qualified certificates for website authentication as in amended regulation 910/2014".
- ETSI EN 319 411-2: "Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".

History

Version	Date	Status
V1.1.1	October 2025	Publication