



**Methods for Testing & Specification (MTS);
Methodology Definition;
Digital Transformation of Security Standards into
Requirements**

get full document from standards.iteh.ai

Reference

DTS/MTS-TST12TraStaReq

Keywords

IoT, LLM, methodology, security

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

Important notice

The present document can be downloaded from the
[ETSI Search & Browse Standards](#) application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on [ETSI deliver](#) repository.

Users should be aware that the present document may be revised or have its status changed,
this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to
the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our
[Coordinated Vulnerability Disclosure \(CVD\)](#) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part of this document may be reproduced in any form, by any means and in any media, without the prior written authorization of ETSI and except as expressly permitted below.

By way of exception and when the document is a normative deliverable (European Standard (EN), Technical Specification (TS), Group Specification (GS) or ETSI Standard (ES)), ETSI authorizes to reproduce and incorporate into products, services and technical documentation only those extracts (e.g. templates) that are strictly necessary for the technical implementation of the normative deliverable, to ensure compliance with the latter. Nothing in this notice shall be construed as limiting any mandatory exceptions to copyright provided by applicable law.

© ETSI 2026.
All rights reserved.

Contents

Intellectual Property Rights	4
Foreword.....	4
Modal verbs terminology.....	4
Executive summary	4
Introduction	5
1 Scope	7
2 References	7
2.1 Normative references	7
2.2 Informative references.....	7
3 Definition of terms, symbols and abbreviations.....	8
3.1 Terms.....	8
3.2 Symbols.....	8
3.3 Abbreviations	9
4 Background	9
5 Methodology Overview.....	9
6 Methodology	10
6.1 Workflow	10
6.2 Adaptation Techniques.....	11
6.3 Document Parsing (DP).....	12
6.4 Requirement Identification and Extraction (RIE).....	12
6.4.1 Fine-tuning.....	12
6.4.1.1 Overview.....	12
6.4.1.2 Dataset Construction and Data Preparation.....	13
6.4.1.3 Model Selection	14
6.4.1.4 Model Evaluation.....	14
6.4.1.5 Model Execution	14
6.4.2 Prompt Engineering	15
6.5 Requirement Classification (RC)	15
6.5.1 Fine-tuning.....	15
6.5.1.1 Overview	15
6.5.1.2 Dataset Construction and Data Preparation.....	15
6.5.1.3 Preprocessing and Model Construction.....	16
6.5.1.4 Model Evaluation.....	16
6.5.1.5 Model Execution	16
6.5.2 Prompt Engineering	16
6.6 Requirement Checklist Generation (RCG).....	17
6.7 Feedback Provision (FP)	17
Annex A (normative): Examples of extracted requirements.....	19
History	23

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables (European Standard (EN), Technical Specification (TS), Group Specification (GS) or ETSI Standard (ES)) 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 Methods for Testing and Specification (MTS).

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.

Executive summary

The present document introduces a methodology for the semi-automated transformation of security standards into a list of security requirements. More specifically, it describes an AI-driven methodology for the identification, extraction, and classification of security requirements from text retrieved from security standards documents. The methodology is based on adapting pre-trained foundational Large Language Models (LLMs) using common adaptation techniques like prompt engineering and fine-tuning in the downstream tasks of security requirements identification, extraction, and classification. The present document can also be used as a guide for practitioners who are interested in utilizing LLMs for automating the identification, extraction, and/or classification of security requirements from security standards.

Introduction

Compliance with international security standards is essential for ensuring the security of digital products and services, and thereby their dependability and trustworthiness. Beyond fostering trust, compliance with security requirements is increasingly mandated by regulatory frameworks in the European Union (EU), such as the Cyber Resilience Act (CRA) [i.1]. In particular, under the CRA, products with digital elements should comply with critical product-level cybersecurity requirements before being placed on the EU market. The CRA entered into force on 10 December 2024, and its main obligations apply from 11 December 2027 (with certain obligations applying earlier). Therefore, compliance with international security standards and regulations has become highly relevant to a broad set of stakeholders and application domains, including some that previously had fewer formal cybersecurity obligations.

Compliance evaluation is typically conducted by security experts (e.g. internal assessors, auditors, etc.) who verify whether critical security requirements expressed in relevant international security standards or regulations are satisfied by the subject system. To state it simply, the security expert works from a list of security requirements that the system needs to satisfy and gathers objective evidence (e.g. technical documentation, test results, etc.) regarding the satisfaction of these requirements. If sufficient evidence is found for the considered requirements, the system can be regarded as fully compliant with the designated/selected security standard or regulation.

Compliance evaluation starts with the extraction of the security requirements that are expressed in a relevant standard or regulation that the system needs to comply with, and their representation in the form of a list of clearly-described and well-structured requirements. Extracting requirements from standards is a tedious, time-consuming, and effort-demanding task, which is also prone to human error. This is mainly attributed to the fact that international security standards are often long documents with complex, highly technical language, requiring technical knowledge and expertise by the person who is tasked to go through their text and detect and extract the security requirements. Until today, this process remains largely manual. Although several rule-based and Natural Language Processing (NLP) techniques have been introduced, they have not achieved the accuracy and generalizability required for broader adoption in practice.

However, the recent advancements in the field of Artificial Intelligence (AI) and particularly the proposition of the Transformer architecture and its derivative LLMs that have demonstrated remarkable capabilities in natural language understanding and processing open a new potential for the automation of the digital transformation process of security standards and regulations.

The present document introduces an AI-based methodology for the semi-automated digital transformation of security standard documents into lists of actionable security requirements, which can be used as the foundation for conducting subsequent compliance evaluation activities. The methodology is based on adapting LLMs in order to be able to:

- i) identify and extract security requirements that are described in the documents of international security standards and regulations;
- ii) categorize/classify them into high-level security criteria/characteristics to which they belong (e.g. Confidentiality, Integrity, Availability, etc.); and
- iii) extract the identified requirements in a unified form, which is both machine- and human-readable.

The methodology for the digital transformation of security standards is based on two separate LLM-based mechanisms, one for the identification and extraction of the security requirements from text retrieved from international security standards and regulations, and another for the classification of the extracted requirements into specific security categories. These two mechanisms are used jointly in order to deliver the desired functionality, acting as independent collaborative AI agents, each one excelling in its designated task and acting synergistically in order to achieve the high-level goal of turning a standard document into a well-structured list (checklist) of security requirements.

The proposed methodology is based on the adaptation of pre-trained foundational LLMs, leveraging common adaptation techniques, including prompt engineering (both zero- and few-shot learning) and fine-tuning. The most suitable adaptation technique needs to be selected for each one of the considered tasks, i.e. requirements identification, extraction, and classification. The present document, apart from the methodology itself, provides guidelines on how to adapt existing LLMs in order to be used as the basis for these important requirements engineering tasks.

The methodology is intended for use by conformity assessment bodies and auditors preparing requirement checklists to be used as the basis for subsequent compliance and certification activities, by product and security engineering teams deriving security requirements from applicable standards, by standards owners and working groups piloting semi-automated requirement-extraction workflows, by tool developers and integrators building LLM-assisted compliance tooling, and by regulators and market-surveillance authorities exploring repeatable methods for requirements derivation.

The present document can be used for deriving a clearly structured set of requirement records from a referenced standard or regulation, configuring and adapting LLMs for requirement identification, extraction and classification, establishing traceability from each derived requirement to the source clause for auditability, supporting human-in-the-loop review and quality control, harmonising internal compliance datasets and processes across products and projects, and benchmarking alternative prompts, models and settings against common acceptance criteria.

The present document is independent of any specific product, vendor, model family, deployment environment or programming framework. It does not prescribe a particular LLM, model size, decoding strategy, training corpus, cloud provider or tooling stack, and it is compatible with both proprietary and open-source implementations, whether deployed on-premises or in cloud environments. Any examples or parameter values are illustrative only and do not imply endorsement. References to external documents are non-exhaustive and provided for context.

Sample Document

get full document from standards.iteh.ai

1 Scope

The present document introduces an AI-driven methodology for enabling the semi-automated transformation of international security standards into a comprehensive list of security requirements. More specifically, the present document specifies a methodology for:

- a) The automatic identification and extraction of security requirements from text retrieved from standard documents.
- b) The classification of security requirements extracted from standards into critical high-level security categories/attributes (e.g. Confidentiality, Integrity, Availability, etc.).
- c) The semi-automated transformation of complete standard documents into a list of well-structured security requirements, incorporating a feedback loop with the user.
- d) Adapting LLMs in the tasks of security requirements identification, extraction and classification.

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.

Not applicable.

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] [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), OJ L, 20.11.2024.
- [i.2] [Object Management Group](#) (2016): "Requirements Interchange Format (ReqIF)", Version 1.2. OMG Document Number formal/2016-07-01.
- [i.3] [ISO/IEC Directives Part 2](#) (Edition 9) (2021): "ISO/IEC Directives, Part 2: 'Principles and rules for the structure and drafting of ISO and IEC documents'", Edition 9, 2021.
- [i.4] Gotel OC, Finkelstein CW: "An analysis of the requirements traceability problem". In Proceedings of IEEE international conference on requirements engineering 1994 Apr 18 (pp. 94-101). IEEE.