ETSI TS 104 170 V1.1.1 (2026-02)

TECHNICAL SPECIFICATION

Cyber Security (CYBER);
Universal Cybersecurity Information Exchange Framework - Repository

Reference
DTS/CYBER-00162

Keywords
cybersecurity

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

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 Cyber Security (CYBER).

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 establishes a design paradigm for openness, diversity, extensibility, and interoperability among cybersecurity resource communities establishing a global decentralised, autonomous framework for sharing structured resource information. The objective is to provide incentives to provide a "connective tissue for sharing." The common resource framework record described in clause 4.2 is both extremely minimal and flexible as well as decentralised and self-replicating on any connected server. It enables any kind of cybersecurity resources to be made known to others in almost any manner and basis of their choosing, including similar lists, specifications, tools and normative bindings. This enables a dynamic and autonomous ensemble of multiple resources including obligation compliance relationships to be discovered and used among different communities. The approach is derived from the newly emerged Global Common Vulnerability and Exposures (GCVE) community that is well-established and scales effectively [i.2].

Introduction

The structured expression of cyber incidents was one of the earliest standards developed among incident reporting teams. Its evolution to exchange vulnerability information and mitigations was a significant next step. The present UCYBEX specification draws upon that work and intended to meet the requirements for a compatible and interoperable common framework that also supports government and industry compliance provisions.

1 Scope

The present document provides a universal, inclusive structured framework-repository directory that identifies cybersecurity activity clusters and associated commonly used specifications that entail information exchange and associated information repositories. Responsible parties, network location and availability are included. Uses involving cybersecurity legislative instruments such as those in the EU, as well as industry norms, are identified and information repositories - especially those used for AI LLM ingestion - are included. The ETSI Forge and OID leaf are used for the UCYBEX repository-directory.

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: "Collaborative tools for standardized technologies".

[2] JSON Schema: "Specification".

[3] IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax".

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] Recommendation ITU-T X.1500: "Overview of cybersecurity information exchange".

[i.2] GCVE.EU: "GCVE: Global CVE Allocation System".

[i.3] EU: "ELI - European Legislation Identifier".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

automation: use of technology, often including AI and machine learning, to automate cybersecurity processes, reducing human intervention and improving the efficiency of security operations

bill of materials: document that lists the software or hardware components, including their versions and dependencies, used in a product or system

coding: knowledge enabling professionals to analyse vulnerabilities, develop security tools, and understand the tactics of malicious actors

configuration: cyber state consisting of the settings, rules and parameters that define enhanced security for a system or network

disinformation: identification of deliberate efforts to spread false information through ICT-based services

hardened images: cyber state consisting of virtual machine images that are pre-configured to meet the robust security recommendations of the associated Critical Security Control Benchmark

incident response: structured process for handling security incidents, including detection, containment, eradication, and recovery

monitoring and auditing: structured process of continuously monitoring systems for security breaches and conducting regular security audits

normative binding: asserted relationship for compliance with one or more obligations in a normative instrument, indicated with an instrument identifier such as a European Legislative Identifier

ontology: set of concepts and categories in a subject area or domain that shows their properties and the relations between them

playbook: standard set of procedures to identify, coordinate, remediate, recover, and track successful mitigations from incidents and vulnerabilities affecting an organisation’s systems, data, and networks

processes: series of steps and procedures designed to protect an organization's assets, data, and systems from cyber threats

risk management: structured process of identifying, assessing, and mitigating cybersecurity risks

risk measurement: quantitative structured process for assessing risk level

security awareness training: process of educating employees about cybersecurity threats and best practices

semantic framework: structured approach to organizing and abstracting data and knowledge, allowing for a deeper understanding of relationships between concepts and entities

state: cybersecurity state of a device or system

threat: malicious action or event that can negatively impact an organization or individual through an information system

trust: means to assess the integrity, security, and reliability of systems, processes, organizations and individuals

vulnerability: specific weakness or flaw in a system, network, or application that attackers can exploit to compromise security

vulnerability management: process of regularly scanning and patching systems for vulnerabilities

weakness: standardized way to describe and classify common software and hardware errors that can be exploited by attackers

3.2 Symbols

Void.

3.3 Abbreviations

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

ELI	European Legislative Identifier
UCYBEX	Universal Cybersecurity Information Exchange Framework

4 Universal Cybersecurity Information Exchange Framework (UCYBEX)

4.0 Cybersecurity information exchange models

The contemporary period of cybersecurity information exchange emerged in the 1990 timeframe and consisted of the exchange of combinations of incident, vulnerability, and threat information via repositories among a complex global community of product and service vendors, end users, and industry and government cyber security organizations [i.1]. The actual sharing of information together with a broad array of related protocols was depicted within ITU-T as a five-component activity. See Figure 4.0-1 below.

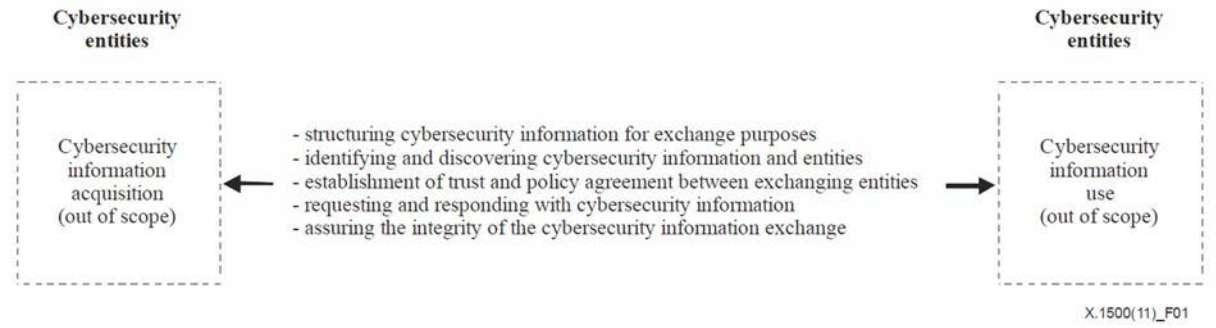

Figure 4.0-1: Cybersecurity information exchange model [i.1]

4.1 UCYBEX Framework - Repository architecture

The present document facilitates the exchange of cybersecurity information using a framework that establishes a design architecture for openness, diversity, extensibility, and interoperability. This global decentralised, autonomous framework architecture enables widespread sharing of cybersecurity resources including obligation compliance relationships via multiple common distributed repositories that enable users to discover and access those resources in the form of other directory lists, specifications, tools, or any other kind of related enrichment information. It is modelled after the Global CVE framework architecture [i.2].

The structure for the framework - repository record format is set forth in clause 4.2. The JSON representation is in Annex A. ETSI Source Forge requirements [1] and JSON format requirements [2] apply to the implementation of the UCYBEX framework. An example of the ETSI implementation of the framework list is provided in Annex B.

4.2 UCYBEX Framework Resource Record Format and Values

4.2.1 Overview

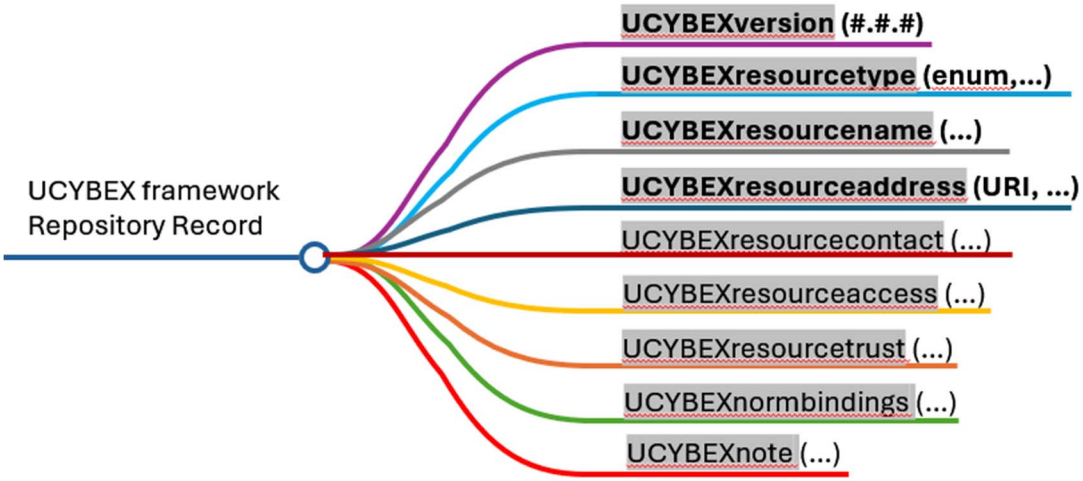

Figure 4.2-1: Mindmap of the UCYBEX Framework Resource Record, V1.0.1

4.2.2 UCYBEXversion

This required value describes the present UCYBEX Framework Resource Record specification version being used and expressed as three numbers separated by commas and set initially to 1.0.1.

4.2.3 UCYBEXresourcetype

This required value describes the UCYBEX resource type in the following non-case-sensitive enumeration:

list	Another UCYBEX or compatible Framework Resource list
spec	Any technical specification for cybersecurity
repository	Any information repository for cybersecurity purposes
enrichment	Any cybersecurity enrichment information including AI BOMs and knowledge graphs
tool	Any program intended to assist cybersecurity or related risk management
playbook	Any playbook for cybersecurity
…	A description of any other resource, preferably using clause 3.1 terminology

4.2.4 UCYBEXresourcename

This required value describes the name of the resource without any constraints - prefaced by any related identifier associated with the name. For example, "ETSI TS 104 170 V1.0.0 - Rec. ITU-T X.1500 Cyber Security (CYBER); Universal Cybersecurity Information Exchange Framework - Repository".

4.2.5 UCYBEXresourceaddress

This required value describes the resource address location without any constraints - preferably as a persistent, precise, accessible Uniform Resource Identifier (URI) or a link capable of providing the resource. For example, https://www.etsi.org/deliver/etsi_ts/104170 [TBD].

4.2.6 UCYBEXresourcecontact

This optional value describes the national incorporation jurisdiction using a recognized country identifier and contact information without any constraints for the entity maintaining and accessing the resource preferably including physical and location and useable email address. For example, "France, ETSI Secretariat, ETSI 650, Route des Lucioles 06560 Valbonne - Sophia Antipolis FRANCE, secretariat@etsi.org".

4.2.7 UCYBEXresourceaccess

This optional value without any constraints describes any resource access controls, for example, "paywall" or "members only". The default when leaving blank is publicly available without constraints.

4.2.8 UCYBEXresourcetrust

This optional value without any constraints describes any resource trust mechanisms such as a digital certificate.

4.2.9 UCYBEXnormbindings

This optional value without any constraints describes any asserted normative binding, i.e. an asserted relationship for compliance with one or more obligations in a normative instrument, indicated with an instrument identifier such as a European Legislative Identifier (ELI) [i.3].

4.2.10 UCYBEXnote

This optional value without any constraints describes any useful attributes of the resource.

Annex A (normative): UCYBEX Framework Resource Record JSON Format V1.0.1

```
{
    "$schema": "http://[tbd]",
    "title": "JSON Schema for UCYBEX Framework Resource Record version 1.0.1",
    "$id": "https://www.etsi.org/[tbd]",
    "properties": {

        "UCYBEXversion": {
            "description": "present UCYBEX Framework Resource Record specification version being
used and expressed as three numbers separated by commas and set initially to 1.0.1",
            "type": "1.0.1"
        },

        "UCYBEXresourcetype": {
            "description": "UCYBEX resource type ",
            "enum": [
             "list",
             "spec",
             "repository",
             "enrichment",
             "tool",
             "playbook"
            ],
            "type": "string",
        },

        "UCYBEXresourcename": {
            "description": "the name of the resource",
            "type": "string",
            "identifier": " ",
            "name": " "
            },

        "UCYBEXresourceaddress": {
            "description": "resource address location",
            "type": "string"
        },

        "UCYBEXresourcecontact": {
            "description": "national incorporation jurisdiction using a recognized country
identifier and contact information for the entity maintaining and accessing the resource",
            "type": "string",
            "jurisdiction": " ",
            "entity name": " ",
            "street": " ",
            "city": " ",
            "phone": " ",
            "email": " "
        },

        "UCYBEXresourceaccess": {
            "description": "describes any resource access controls",
            "type": "string"
        },

        "UCYBEXresourcetrust": {
            "description": "any resource trust mechanisms",
            "type": "string"
        },

        "UCYBEXresourcenormbindings": {
            "description": "any asserted normative binding, i.e. an asserted relationship for
compliance with one or more obligations in a normative instrument",
            "type": "string"
        },

        "UCYBEXnote": {
            "description": "any useful attributes of the resource",
            "type": "string"
        },
```

```
    },
    "required": [
     "UCYBEXversion",
     "UCYBEXresourcetype",
     "UCYBEXresourceaddress"
     ]
}
```

Annex B (informative): ETSI UCYBEX Framework Resource Record Example

UCYBEXversion	1.0.1
UCYBEXresourcetype	spec
UCYBEXresourcename	ETSI TS 104 170 V1.0.1 , Cyber Security (CYBER); Universal Cybersecurity Information Exchange Framework - Repository
UCYBEXresourceaddress	https://www.etsi.org/deliver/etsi_ts/104170[TBD]
UCYBEXresourcecontact	France, ETSI Secretariat, ETSI 650, Route des Lucioles 06560 Valbonne - Sophia Antipolis FRANCE, secretariat@etsi.org
UCYBEXresourceaccess	
UCYBEXresourcetrust	Certificate, fdfad996ee0874b568dc40b300ec036d91456150b1acfaf69c25b2bb13f55483
UCYBEXnormbindings	
UCYBEXnote	ETSI implementation specification for UCYBEX framework resource repository
=====	
UCYBEXversion	1.0.1
UCYBEXresourcetype	repository
UCYBEXresourcename	UCYBEX Framework Resources Known to ETSI
UCYBEXresourceaddress	https://forge.etsi.org/rep/explore/projects [TBD]
UCYBEXresourcecontact	France, ETSI Secretariat, ETSI 650, Route des Lucioles 06560 Valbonne - Sophia Antipolis FRANCE, secretariat@etsi.org
UCYBEXresourceaccess	
UCYBEXresourcetrust	Certificate, fdfad996ee0874b568dc40b300ec036d91456150b1acfaf69c25b2bb13f55483
UCYBEXnormbindings	
UCYBEXnote	ETSI implementation of UCYBEX resource framework repository
=====	
UCYBEXversion	1.0.1
…..	

Annex C (informative): Bibliography

- ML Commons: Croissant.
- Schema.org: Schemas.

History

Version	Date	Status
V1.1.1	February 2026	Publication