



**Securing Artificial Intelligence (SAI);
AI Incident Reporting;
Part 1: AI Common Incident Expression (AICIE)
Global Framework**

get full document from standards.iteh.ai

Reference

DTS/SAI-0020

Keywords

artificial intelligence, 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

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 may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2026.
All rights reserved.

Contents

Intellectual Property Rights	4
Foreword.....	4
Modal verbs terminology.....	4
Executive summary	4
Introduction	5
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	6
3 Definition of terms, symbols and abbreviations.....	8
3.1 Terms.....	8
3.2 Symbols.....	9
3.3 Abbreviations	9
4 Existing Ecosystem	9
4.1 Cybersecurity information exchange models	9
4.2 AI incident information exchange implementations.....	10
4.3 AI Incident information exchange obligations	10
4.3.1 The exchange obligation ecosystem	10
4.3.2 EU Artificial Intelligence Act.....	11
4.3.3 ETSI TS 104 223, UK DSIT Code of Practice	12
5 AI Common Incident Expression (AICIE) Framework	13
5.1 The AICIE Framework architecture	13
5.2 AICIE Framework Resource Record Format and Values	13
5.2.0 Introduction.....	13
5.2.1 AICIEresource	13
5.2.2 AICIEresource type	14
5.2.3 AICIEresource name.....	14
5.2.4 AICIEresource address	14
5.2.5 AICIEresource contact.....	14
5.2.6 AICIEresource access	14
5.2.7 AICIEresource add	14
Annex A (normative): AICIE Framework Resource Record JSON Format V1.0.1.....	15
Annex B (informative): ETSI AICIE Framework Resource Record Example	16
Annex C (informative): Bibliography	17
History	18

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 Securing Artificial Intelligence (SAI).

The present document is part 1 of a multi-part deliverable covering AI Incident Reporting, as identified below:

Part 1: "AI Common Incident Expression (AICIE) Global Framework";

Part 2: "AI Common Incident Expression (AICIE) Common Container";

Part 3: "AI Common Incident Expression (AICIE) Security Container".

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 technical specification establishes a design paradigm for openness, diversity, extensibility, and interoperability among AI reporting communities by creating a first part establishing a global decentralised, autonomous framework for sharing structured AI incident information. The objective is described as a framework designed to provide incentives to collaborate on AI incidents and exist as "connective tissue for sharing."

The preparation of the present document made clear that there was a basic bifurcation existed between the needs of AI incident information for "AI safety" and for "AI security". It was also clear that the requirements would be constantly evolving and that three different user communities existed:

- 1) third-party incident information collectors;
- 2) sovereign repository instantiations by government authorities; and
- 3) companies with AI offerings dealing with vulnerabilities and security.

The common resource framework record described in Clause 5.2 is both extremely minimal and flexible as well as decentralised and self-replicating on any connected server. It enables any kind of AI incident related resources to be made known to others in almost any manner and basis of their choosing, including similar lists, specifications, and repositories of information "containers". This enables a dynamic and autonomous ensemble of multiple AI reporting standards, exchange mechanisms and repositories to emerge and communicate 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.

A subsequent part of the present document provides a specification for a generic common incident reporting data record container derived from work of the OECD and other current providers of AI incident reporting.

Introduction

The OECD published in 2025 a significant report that summarized several years of study by itself and numerous other organizations urging a Common Framework for AI Incident Reporting. See [i.10] and in Annex C (Bibliography). The OECD structure is reflected in the container specification in ETSI TS 104 158-2 [i.33]. Implementing this capability is a matter of some substantial interest to the European Commission as its Artificial Intelligence AI Act requires several incident reporting actions. See [i.2]. Incident reporting requirements are also instantiated in NCSC AI security guides and Commonwealth legislative instruments and ETSI's own Baseline Cyber Security Requirements for AI Models and Systems [i.1].

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 AI Common Incident Expression (AICIE) 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.

The AI Common Incident Expression Framework in the present document is intended to support very diverse kinds of AI incident resources and communities of interest, threats, and threat actors that go well beyond the cybersecurity domain. It makes use of a decentralised open architecture pioneered by the Global CVE community supported by the CIRCL Computer Incident Response Center Luxembourg. See [i.8]. Specifying the present framework designs for openness, diversity, extensibility, and interoperability. This approach enables a dynamic and autonomous ensemble of other AI reporting standards, exchange mechanisms and repositories to emerge and communicate among different user communities.

ETSI TS 104 158-2 [i.33] provides an AI incident reporting information container. It consists of a generic common incident reporting data record container based on the OECD reporting model structure.