



**Securing Artificial Intelligence (SAI);
AI Incident Reporting;
Part 2: AI Common Incident Expression (AICIE)
Common Container**

get full document from standards.iteh.ai

Reference

DTS/SAI-0027

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
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.....	8
3.3 Abbreviations	8
4 AICIE Common Container Record	8
4.1 AICIE Common Container Record Format and Values	8
4.1.1 Introduction.....	8
4.1.2 AICIECCversion.....	9
4.1.3 AICIECCtitle	9
4.1.4 AICIECCincidentDescription	10
4.1.5 AICIECCsystemRelationship	10
4.1.6 AICIECCsubmitterInformation	10
4.1.7 AICIECCdateFirstOccurred.....	10
4.1.8 AICIECCincidentCountry	10
4.1.9 AICIECCincidentMaterial	10
4.1.10 AICIECCaiProduct	10
4.1.11 AICIECCaiSystemDeveloper	10
4.1.12 AICIECCseverity.....	11
4.1.13 AICIECCcharmType	11
4.1.14 AICIECCcharmConsequence	11
4.1.15 AICIECCintentionality	11
4.1.16 AICIECCpartiesAffected.....	11
4.1.17 AICIECChumanRightsImpact	12
4.1.18 AICIECCprinciplesAffected.....	12
4.1.19 AICIECCindustry	12
4.1.20 AICIECCbusinessFunction.....	12
4.1.21 AICIECCcriticalInfrastructure.....	12
4.1.22 AICIECCdeploymentBreadth.....	13
4.1.23 AICIECCtrainingDataLink	13
4.1.24 AICIECCincidentModelLink.....	13
4.1.25 AICIECCusageRights	13
4.1.26 AICIECCmultipleSystems.....	13
4.1.27 AICIECCaiTasks	14
4.1.28 AICIECCautonomyLevel	14
4.1.29 AICIECCactionTaken.....	14
4.1.30 AICIECCstepsReproduced	14
4.1.31 AICIECCadditionalInfo	14
Annex A (normative): AICIE Common Container JSON record Format V1.0.1.....	15
Annex B (informative): Common reporting framework recommendations	20
History	23

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 2 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.

Introduction

The common resource framework record described in Part 1 of the present document (ETSI TS 104 158-1 [1]) 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."

Part 1 (ETSI TS 104 158-1 [1]) enables many different containers. Most of the information fields optional. The present part of the present document provides for a generic data record for an AICIE "common container" derived from work of the OECD, published government and industry requirements, and other current researchers and providers of AI incident reporting that attempts to bridge the highly diverse reporting and user communities [i.1] thru [i.33].

Sample Document

get full document from standards.iteh.ai

1 Scope

The present document provides a technical specification for an AI Common Incident Expression Common Container for AI Incident Reporting.

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 TS 104 158-1](#): "Securing Artificial Intelligence (SAI); AI Incident Reporting; Part 1: AI Common Incident Expression (AICIE) Global Framework".

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 TS 104 223 \(V1.1.1\)](#): "Securing Artificial Intelligence (SAI); Baseline Cyber Security Requirements for AI Models and Systems".
- [i.2] [Regulation \(EU\) 2024/1689](#) of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).
- [i.3] UK DSIT: "[AI Cyber Security Code of Practice](#)".
- [i.4] UK NCSC: "[Guidelines for secure AI system development](#)".
- [i.5] [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.6] [Commission Implementing Regulation \(EU\) 2024/2690](#) of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers.
- [i.7] [Directive \(EU\) 2022/2557](#) of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.
- [i.8] GCVE.EU: "[GCVE: Global CVE Allocation System](#)".
- [i.9] Sean McGregor, et al. (2025): "[In-House Evaluation Is Not Enough: Towards Robust Third-Party Flaw Disclosure for General-Purpose AI](#)", Cornell University SarXiv:2503.16861v1 [cs.AI].
- [i.10] OECD: "[Towards a Common Reporting Framework for AI Incidents](#)", OECD Artificial Intelligence Papers, February 2025, No. 34.
- [i.11] OECD: "[AIM: AI Incidents and Hazards Monitor](#)".
- [i.12] OECD: "[Defining AI Incidents and Related Terms](#)", OECD Artificial Intelligence Papers, May 2024, No. 16.
- [i.13] McGregor, S. (2021): "[Preventing Repeated Real World AI Failures by Cataloging Incidents: The AI Incident Database](#)", Proceedings of the AAAI Conference on Artificial Intelligence, 35(17), 15458-15463.
- [i.14] OECD: "[OECD Framework for the Classification of AI Systems](#)", OECD Digital Economy Papers, February 2022, No. 323.
- [i.15] NCSC: "[Where to Report a Cyber Incident](#)".
- [i.16] NCSC: "[Responding to a cyber incident - a guide for CEOs](#)".
- [i.17] Confédération Suisse, Federal Office for Cybersecurity BACS: "[Information on the reporting obligation](#)".
- [i.18] H. Frase, R.B. L. Dixon: "[AI Incidents. Key Components for a Mandatory Reporting Regime](#)", CSET, January 2025.
- [i.19] [OWASP Gen AI Incident/Exploit Round-up Submission](#).
- [i.20] [Recommendation ITU-T X.1500](#): "Overview of cybersecurity information exchange".
- [i.21] [ETSI TR 104 003](#): "Cyber Security (CYBER); The vulnerability disclosure ecosystem".
- [i.22] [ETSI TR 103 331](#): "Cyber Security (CYBER); Structured threat information sharing".
- [i.23] CISA: "[Cybersecurity Incident & Vulnerability Response Playbooks](#)".
- [i.24] [NIST AI 600-1](#): "Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile".
- [i.25] AIID: "[AI Incident Database](#)".
- [i.26] MIT: "[AI Risk Repository](#)".
- [i.27] AVID: "[AI Vulnerability Database](#)".
- [i.28] OECD: "[Overview and methodology of the AI Incidents and Hazards Monitor](#)".
- [i.29] Partnership on AI: "[AI Incident Database](#)".
- [i.30] Kaggle: "[AI Incident Database](#)".