International Standard

ISO/IEC 5181

Information security, cybersecurity and privacy protection — Data provenance

Sécurité de l'information, cybersécurité et protection de la vie privée — Provenance des données

First edition
2026-10

Reference number
ISO/IEC 5181:2026(en)

© ISO/IEC 2026

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Abbreviated terms ... **5**
5 Data provenance methodology ... **6**
5.1 General assumptions ... 6
5.2 Verification and validation principles ... 7
5.3 Value stream semantics ... 8
5.3.1 Correspondence between LC value streams ... 8
5.3.2 Value stream behaviour ... 8
5.3.3 Representation of VS semantics ... 9
5.3.4 Continuity aspect of operating products and data ... 10
5.3.5 Formal language terms ... 10
5.3.6 Processing of trust ... 10
5.3.7 Quality of data provenance ... 11
5.4 Value stream description language ... 11
5.4.1 Using variables ... 11
5.4.2 Data provenance proposition ... 11
5.4.3 Catalogue of narrative of provenance artefacts ... 12
5.4.4 Generating a narrative of provenance by example ... 13
6 Data provenance information model ... **14**
6.1 General ... 14
6.2 Data flow control model ... 14
6.3 Data provenance complexity model ... 14
6.4 Data provenance reference architecture model ... 15
6.5 Data provenance security and privacy model ... 16
Annex A (informative) **DP artefacts of narrative of provenance** ... **18**
Annex B (informative) **Operational ontology of DP** ... **23**
Annex C (informative) **Dataspaces for data provenance** ... **25**
Annex D (informative) **Data provenance constraints derived from regulations** ... **27**
Bibliography ... **28**

© ISO/IEC 2026 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

© ISO/IEC 2026 – All rights reserved

Introduction

This document provides guidelines and methods on how to derive data provenance information from a system of co-operating authenticated stakeholders. Data provenance is valid if, the data value stream represented by sequences of < data, metadata > tuples, in any life cycle phase of compound industrial data and production value streams, is always comparable to the value stream of production involving operational technology. Hence, the < data, metadata > tuples value stream is twinning the production value stream such that both data and production value streams are isomorphic to each other.

The use and processing of data performed by applications, systems, robots, individuals, agents or companies usually is subject of permissions from data owners as applied in ISO/IEC 62890.[23]

“Data owner” is a term that is applied to the rights of a data holder. Data holders have the rights to access, use, or manipulate their data. The data owner role is understood as an individual or a group of stakeholders who can have control over certain data attributes like data creation, accuracy or the names or identifiers of sources, etc.

Data provenance information is useful to all who want to use available data in other applications or want to decide to make data voluntarily available as a common good in a dataspace that can be subscribed by various application stakeholders. Identifying and deriving information from the history of metadata events provide details on the narratives of data provenance and data manipulations. The concept of narration is used because it visually describes sequences of activities or the state changes of a system. Graphically, a sequence of state changes or events is a graph trajectory.

© ISO/IEC 2026 – All rights reserved

Information security, cybersecurity and privacy protection — Data provenance

1 Scope

This document provides guidelines, methodologies and techniques for securely deriving information about data assets from multiple sources, intermediaries or users, which is denoted as provenance metadata.

2 Normative references

Bibliography

[1] ISO/IEC 30141:2024, *Internet of Things (IoT) — Reference architecture*

[2] ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*

[3] ISO/IEC 29100:2024, *Information technology — Security techniques — Privacy framework*

[4] Freeman, Hupfer, Arnold: JavaSpaces™ Principles, patterns, and Practices, The Jini Technology Series, 1999 Sun Microsystems Inc.

[5] Zohar Manna, Richard Waldinger: The logic basis for Computer Programming, Volume 1 Deductive Reasoning, Addison Wesley 1985

[6] Joint Technical Report of DCKN TEG AAS/DTw/UCA on Digital Data Chain Consortium (DDCC) Integrating Data Technologies on the Information Exchange Platform (IEP)

[7] ISO/IEC/TS 5723:2022, *Trustworthiness — Vocabulary*

[8] ISO/IEC 20803, *Cards and Security Devices for personal identification – Interindustry Mechanism of data credibility enhancement with personal identification and authentication*

[9] ISO/IEC 20151-1:—[3], *Cloud computing and distributed platforms — Dataspaces — Part 1: Concepts and characteristics*

[10] VDE SPEC 90009 v1.0, Meta-metadata for technical documentation in Industry 4.0, inspected 2024-12-28, available at:[4]

[11] Gaia-X EU Association for Data and Cloud AISBL Glossary 31, Dataspace is a decentralized governed structure to enable trustworthy data-sharing between DS participants on a voluntary basis.

[12] W3C.org Provenance WG - An overview of the PROV Family of documents defining aspects necessary to achieve interoperable interchange of provenance information in heterogeneous environments

[13] IEC 61360-1, *Standard data element types with associated classification scheme – Part 1: Definitions - Principles and methods*

[14] C2PA technical specifications for providing content provenance and authenticity as presented by C2PA.org[5]

[15] Ko, R.K.L., Phua, T.W. (2017) describe 'The Full Provenance Stack: Five layers for complete and meaningful provenance' published in: Wang, G., Atiquzzaman, M., Yan, Z., Choo, KK. (eds) 'Security, Privacy, and Anonymity in Computation, Communication, and Storage', SpaCCS 2017, Lecture Notes in Computer Science, vol 10658. Springer, Cham. https://doi.org/10.1007/978-3-319-72395-2_18

[16] ISO/TR 9814:2025, *Ships and marine technology – Good practices of preventing capsizing during turning of ships with large profile height*

[17] ITU-T SG13 Y.3602, *Big data – functional requirements for data provenance, inspected 2024-12-28*[6]

[18] ISO/IEC/TS 30149, *Internet of Things (IoT) — Trustworthiness principles*

[19] ISO/IEC 11179-3:2023, *Information technology — Metadata registries (MDR) — Part 3: Metamodel for registry common facilities*

3) Under development. Stage at the time of publication: ISO/IEC FDIS 20151-1:2026.

4) https://www.ec-systems.de/en/news/042022-vde-spec-90009/

5) https://c2pa.org/specifications/specifications/2.0/specs/C2PA_Specification.html

6) https://handle.itu.int/11.1002/1000/15074

© ISO/IEC 2026 – All rights reserved

[20] ISO/IEC 11179-3:2023/Amd 1:2026, *Information technology — Metadata registries (MDR) — Part 3: Metamodel for registry common facilities — Amendment 1: Enhancements to Item Mapping*

[21] ISO/IEC 11179-33, *Information technology — Metadata registries (MDR) — Part 33: Metamodel for data set registration*

[22] ISO/IEC 25012, *Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Data quality model*

[23] ISO/IEC 62890, *Industrial-process measurement, control and automation – Life cycle management for systems and components; Data.europa.deu: What is data ownership, and does it still matter under EU data law? (last inspection 25-02-16)*

[24] IEC 63278-4:—[7], *Asset administration shell for industrial applications – Part 4: Use cases and modelling examples*

[25] ETSI RFC 8610, *Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures, inspected 2025-01-01*[8]

[26] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), available at: https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng

[27] ISO/TR 14872:2025, *Health informatics — Identification of medicinal products — Core principles for maintenance of identifiers and terms*

[28] ISO/IEC 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

[29] ISO/IEC TR 24800-1:2012, *Information technology — JPSearch — Part 1: System framework and components*

[30] DKE library 931-1_2023-0065 ICT products and ICT services supply chain security

[31] IEC 62443 (all parts), *Requirements and processes for implementing and maintaining electronically secure industrial automation and control systems (IACS)*

[32] Phenological vocabulary, available at: https://www.vocabulary.com/dictionary/phenological, accessed 17. Apr. 2025

[33] ISO/IEC 30194:2024, *Internet of things (IoT) and digital twin — Best practices for use case projects*

[34] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng

[35] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), available at: https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng

7) Under preparation. Stage at the time of publication: IEC/FDIS 63278-4.

8) https://datatracker.ietf.org/doc/html/rfc8610

© ISO/IEC 2026 – All rights reserved