IEEE SA
STANDARDS ASSOCIATION

IEEE Standard for Machine Readable Personal Privacy Terms

STANDARDS

IEEE Society on Social Implications of Technology

Developed by the
Social Implications of Technology Standards Committee

IEEE Std 7012™-2025

IEEE

IEEE Standard for Machine Readable Personal Privacy Terms

Developed by the

Social Implications of Technology Standards Committee
of the
IEEE Society on Social Implications of Technology

Approved 4 November 2025

IEEE SA Standards Board

Abstract: Contractual interactions and agreements between individuals and the service providers they engage on a network, including websites, applications and AI agents, are covered in this standard. It describes how individuals, acting as first parties, can proffer their privacy requirements as contractual terms and arrive at agreements recorded and kept by both sides. These terms shall be chosen from a collection of standard-form agreements in a roster kept by an independent and neutral non-business entity.(This is similar to how artists might choose Creative Commons licenses allowing or restricting certain kinds of uses for artists' creative work.) Computing devices and software performing as agents for both first and second parties shall engage using any protocol that serves the purpose. The first party shall point to a preferred agreement, or a set of agreements, from which the second party shall accept one. Party-to-party negotiations over terms in any of these contracts or other agreements are outside the scope of this standard. If both parties agree, the chosen contract or agreement shall be signed electronically by both parties or their agents, and a matching record shall be kept by both sides in a form that can be retrieved, audited, or disputed, if necessary, at some later time—and which is available to do so easily.

Keywords: automation, ethics, IEEE 7012™, machine-readable, privacy, terms and conditions, transparency

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

PDF: ISBN 979-8-8557-2944-3 STD28515
Print: ISBN 979-8-8557-2945-0 STDPD28515

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (https://standards.ieee.org/ipr/disclaimers.html), appear in all IEEE standards and may be found under the heading "Important Notices and Disclaimers Concerning IEEE Standards Documents."

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents are developed within IEEE Societies and subcommittees of IEEE Standards Association (IEEE SA) Board of Governors. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers involved in technical working groups are not necessarily members of IEEE or IEEE SA and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning all standards, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement IEEE Standards documents do not guarantee safety, security, health, or environmental protection, or compliance with law, or guarantee against interference with or from other devices or networks. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. IEEE Standards documents are supplied "AS IS" and "WITH ALL FAULTS."

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document should rely upon their own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus balloting process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English language version published by IEEE is the approved IEEE standard.

Use by artificial intelligence systems

In no event shall material in any IEEE Standards documents be used for the purpose of creating, training, enhancing, developing, maintaining, or contributing to any artificial intelligence systems without the express, written consent of IEEE SA in advance. "Artificial intelligence" refers to any software, application, or other system that uses artificial intelligence, machine learning, or similar technologies, to analyze, train, process, or generate content. Requests for consent can be submitted using the Contact Us form.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual is not, and shall not be considered or inferred to be, the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE or IEEE SA. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group. Statements made by volunteers may not represent the formal position of their employer(s) or affiliation(s). News releases about IEEE standards issued by entities other than IEEE SA should be considered the view of the entity issuing the release rather than the formal position of IEEE or IEEE SA.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents**.

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its Societies and subcommittees of the IEEE SA Board of Governors are not able to provide an instant response to comments or questions, except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in evaluating comments or revisions to an IEEE standard is welcome to join the relevant IEEE SA working group. You can indicate interest in a working group using the Interests tab in the Manage Profile & Interests area of the IEEE SA myProject system.[1] An IEEE Account is needed to access the application.

Comments on standards should be submitted using the Contact Us form.[2]

[1] Available at: https://development.standards.ieee.org/myproject-web/public/view.html#landing.
[2] Available at: https://standards.ieee.org/about/contact/.

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not constitute compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

Copyrights

Photocopies

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit IEEE Xplore or contact IEEE.[3] For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE SA Website.[4] Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in IEEE Xplore. Users are encouraged to periodically check for errata.

Patents

IEEE standards are developed in compliance with the IEEE SA Patent Policy.[5]

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at https://standards.ieee.org/about/sasb/patcom/patents.html. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

IMPORTANT NOTICE

Technologies, application of technologies, and recommended procedures in various industries evolve over time. The IEEE standards development process allows participants to review developments in industries, technologies, and practices, and to determine what, if any, updates should be made to the IEEE standard. During this evolution, the technologies and recommendations in IEEE standards may be implemented in ways not foreseen during the standard's development. IEEE standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, data privacy, and interference protection practices and all applicable laws and regulations.

[3] Available at: https://ieeexplore.ieee.org/browse/standards/collection/ieee.
[4] Available at: https://standards.ieee.org/standard/index.html.
[5] Available at: https://standards.ieee.org/about/sasb/patcom/materials.html.

Participants

At the time this standard was completed, the Machine Readable Privacy Terms Working Group had the following membership:

Doc Searls, *Chair*
Justin Byrd, *Vice Chair*
Mary Hodder, *Editor*
Scott Mace, *Secretary*

Rob Aaron
Bernd Blobel
Salvatore D'Agastino
Beatriz Esteves
Daniel Hardman
Iain Henderson
Lisa LeVasseur
Vikas Malhotra
Thomas Mahon
Harshvardhan J. Pandit
James Pasquale
Reza Rassool
David P. Reed
Joseph Savirimuthu
Joyce Searls
Steve Vitka
John Wunderlich

The following members of the individual Standards Association balloting group voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Boon Chong Ang
Justin Byrd
Zhiman Chen
Hassan El Shazly
A. Ferraro
Deborah Hagar
Mary Hodder
Werner Hoelzl
Tyler Jaynes
Piotr Karocki
Quist-Aphetsi Kester
Ruth Lewis
Daozhuang Lin
Weili Liu
Scott Mace
Howard Penrose
R. K. Rannow
Jhony Sembiring
Chandra Shekhar Sharma
Robert Spence
Walter Struppler
Stephen Webb
Peter Wishart

When the IEEE SA Standards Board approved this standard on 4 November 2025, it had the following membership:

Lei Wang, *Chair*
Jon Walter Rosdahl, *Vice Chair*
David J. Law, *Past Chair*
Alpesh Shah, *Secretary*

Edward Au
Ted Burse
Xiaofeng (Alfred) Chen
Doug Edwards
Nehad El-Sherif
J. Travis Griffith
Deborah R. Hagar
Guido R. Hiertz
Ronald W. Hotchkiss
Tyler L. Jaynes
Thomas Koshy
Howard Li
Xiaohui Liu
Kevin W. Lu
Hiroshi Mano
Daleep C. Mohla
Annette D. Reilly
Robby Robson
Daniel Sabin
F. Keith Waters
Sha Wei
Luyang (Eric) Zhang

Introduction

This introduction is not part of IEEE Std 7012-2025, IEEE Standard for Machine Readable Personal Privacy Terms.

Privacy in business has always been based on a consensus about how people and corporate entities respect each other's boundaries. This consensus takes the form of tacit agreements about how people signal and respect perceived privacy needs. Clothing, for example, is a technology that protects a person's private regions, both by covering those regions and signaling a boundary against unwelcome observation and approach. Doors, curtains, and shutters are also well understood as privacy technologies that cover spaces and signal degrees of welcome. An extended hand is a signal from one person to another that opens communication that may involve additional gestures about privacy needs that both parties understand—but at a tacit level, meaning well known but not easy to explain. The online world, however, is entirely digital. Signals and rules must be explicit for hardware and software to act on them. Privacy signals therefore must be made explicit: stated in code and respected by code. To make these explicitly coded agreements, they can take the form expressed in contracts, which two parties make for themselves: a form agreement that can be expressed as computer code.

It is helpful that contractual interactions have been well-established online throughout the first quarter of the 21st century. Signaling during this time, however, has been largely from the corporate side, using a routine called "notice and consent." This routine was already *pro forma* in business across many decades before the Internet appeared. In a landmark 1943 paper titled "Contracts of Adhesion: Some Thoughts About Freedom of Contract" [B28],[6] Friedrich Kessler described standard-form business agreements ("contracts of adhesion") as ones in which the customer, being the weaker party, had no choice but to acquiesce and agree. He described the proffering and signing of these agreements as "ceremonies" in which the "deliberate nature of a transaction (is) reduced to the absolute minimum." He also saw these contracts as an unfortunate requirement for companies to obtain scale across countless customers. He lamented that freedom of contract—long a bedrock principle of open societies and free market economies—was in the industrial age available to companies alone, and not to customers when dealing with companies.

Kessler, however, did not anticipate digital technology or the Internet: a "network of networks" that puts everyone and everything on it at a functional distance apart of zero. Nor did he imagine that such a network would be based on equity between the entities on it,[7] and on which freedom of contract could be rebuilt.

The Internet's base protocols (TCP/IP) guide the movement of packetized data from any one end to any other end without prejudice toward the contents of data packets, the paths over which packets are routed, or who owns or controls any of the paths or routing points. TCP/IP also supports other protocols (e.g., HTTP) that are equally equitable by design. These open and equitable protocols by design also support freedom of contract between any two parties. This means any person can have as much free and open contractual scale across corporate entities as corporate entities have long had across people. At least one such contract[8] has been available since 2017 as a collection of personal privacy agreements in "human-readable" text and legal code. To achieve machine readability and the framework in which persons can operate as first parties in contractual engagements online, or to do so at scale, requires a standard.

In their 2013 paper, "Beyond Notice and Choice: Privacy, Norms, and Consent," [B35] Robert H. Sloan and Richard Warner write, "A fundamental difficulty is the lack of norms. Rapid advances in information processing technology have fueled new business models, and the rapid development has outpaced the slow evolution of norms. Notice and Choice cannot be pressed into service to remedy this lack. It is necessary to develop new norms."

[6] The numbers in brackets correspond to those of the bibliography in Annex E.
[7] "End to end encryption," https://web.archive.org/web/20240722165617/https://www.cybertelecom.org/notes/end_to_end.htm.
[8] The #NoStalking agreement is available at Customer Commons, which was formed in 2013 to host a collection of personal privacy agreements, much as Creative Commons hosts a collection of personal copyrights. As with Creative Commons licenses, #NoStalking is expressed in "human-readable" text and legal code. https://customercommons.org/p7012/p2b1

In the absence of a norm, regulations may be inadequate. The "consent notice" system, which appears when one arrives at many websites for the first time, arose at least partly in response to the European Union's General Data Protection Regulation (GDPR) [B9], which became enforceable on 25 May 2018. While the purpose of the GDPR was to provide privacy to persons on networks, website operators and other service providers managed to keep their tracking-based advertising business going.[9] This gave rise to notice and consent choices that made it easy for persons to click on an "agree" (or similar) button that allowed offsite tracking and sale or sharing of personal data with other parties.[10]

The cost to website and service operators of maintaining consent notices and records of GDPR compliance is also high. So is cognitive overhead on both sides that did not exist before the GDPR's enforcement date. The California Consumer Privacy Act (CCPA) [B3], which became enforceable on January 1, 2020, added additional operational and cognitive overhead for everyone by adding a clickable "Do Not Sell or Share" option to websites.[11]

Do Not Track (DNT) became a W3C working group in 2011 [B7]. The title morphed into "Tracking Preference Expression," [B37] and the group disbanded on January 19, 2019. Global Privacy Control (GPC) [B11], another standard in development at the W3C, specifies requests that may be sent by browser headers to websites, and which website operators can obey or ignore at their discretion. These requests are not agreements and can leave the person (a mere "user") in a nearly powerless position. While such programs may be ethically laudable, they leave the person in a subordinate position, with privacy provided as a grace rather than as a fully respected personal requirement.

The Digital Markets Act in the European Union [B6], which came into force in 2024, aims to increase competition among platform providers and limit the ability of the largest providers (which it calls "gatekeepers") to control whole markets. It does not address the need for individual persons to express or command obedience to their privacy requirements.

A framework in which persons can operate as parties in contractual engagements online can solve the problem of absent equity between persons and other entities and improve respect for personal privacy requirements.

Acknowledgements

The working group acknowledges the American National Standards Institute (ANSI) who, on behalf of the International Organization for Standardization granted permission for the use of definitions from ISO 22600-2:2014 and figures from ISO23903:2021. All rights reserved.

The working group acknowledges Health Seven® International for granting permission to reprint the Logical Data Model in Annex D.

[9] This is a system Shoshana Zuboff calls "surveillance capitalism." [B32].

[10] These one-sided contracts of adhesion are presented as non-negotiable terms of service that sometimes offer a small set of secondary choices absent of any way for the person to access the agreement, or to audit for compliance, or to dispute, because the corporate entities and their third parties keep all records of agreements and provide no means for easy access by individual counterparties.

[11] As with the GDPR, sites and services offering the CCPA option provide no means for the individual to access the agreement, to audit for compliance, or to dispute. While the CCPA does afford persons a set of rights, none take effect before the person acts, such as by requesting copies of collected personal information. There are, however, no standard ways for persons to do that or for companies to comply. While the law does allow "authorized agents" (such as Consumer Reports through its Permission Slip phone app), there is still no way a person can obtain a signed agreement respecting their personal privacy, or to do so at scale.

Contents

IEEE Standard for Machine Readable Personal Privacy Terms

1. Overview

Establishing agreements proffered by individuals entails a new kind of "service negotiation," which can be simple and straightforward, or complex with multiple iterations.

1.1 Scope

The standard identifies/addresses the manner in which personal privacy terms are proffered and how they can be read and agreed to by machines.

The scope of this draft standard is confined to routines in which persons acting as first parties arrive at contractual agreements with organizational entities acting as second-party service providers. It is limited to the selection and signing of a contract kept in a public roster by a neutral noncommercial entity, with identical copies of that contract kept by both parties.

1.2 Purpose

The purpose of the standard is to provide individuals with means to proffer their own terms respecting personal privacy, in ways that can be read, acknowledged and agreed to by machines operated by others in the networked world. In a more formal sense, the purpose of the standard is to enable individuals to operate as first parties in agreements with others—mostly companies—operating as second parties.

1.3 Extant standards and regulations

Operation of this standard depends on the Internet Protocol Suite, especially TCP/IP, and HTTP. Also, while this standard does not depend on extant regulations, it may prove to help those regulations by bringing contracts into the suite of available ways to provide personal privacy on networks.

1.4 Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).[12,13]

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

2. Normative references

There are no normative references for this draft standard. There are many useful informative references, however, in the Bibliography (Annex E).

3 Definitions

3.1 Definitions

For the purposes of this document, the following terms *and definitions apply. The IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.[14]

agent: An agent is an actor that works on behalf of a person to represent them, to present proposed terms and agreements to entities, and to store finalized contracts and metadata about terms, agreements and contracts between persons and counterparties.

agent-agreement: An agent generated agreement is presented to an entity on behalf of an individual who has chosen their preferred terms.

agreement: An agreement is a compound set of terms or clauses, proposed and offered before a formal contract between parties, sometimes referred to as a "proposal" or "proposed agreement."

agreement-chooser: An agreement-chooser in an agent allows a person to choose, or delegate to a trusted party, structured, compound sets of terms or clauses.

contract: A contract is a mutual agreement between parties that creates mutual obligations and is enforceable by law.

[12] The use of the word *must* is deprecated and cannot be used when stating mandatory requirements; *must* is used only to describe unavoidable situations.
[13] The use of *will* is deprecated and cannot be used when stating mandatory requirements; *will* is only used in statements of fact.
[14] *IEEE Standards Dictionary Online* is available at: http://dictionary.ieee.org. An IEEE account is required for access to the dictionary, and one can be created at no charge on the dic*tionary sign-in page.*

Data Privacy Vocabulary (DPV): Enables expressing machine-readable metadata about the use and processing of (personal or otherwise) data and technologies based on legislative requirements such as the General Data Protection Regulation (GDPR).]

entity: Any organization with which a person makes a contractual agreement. An entity can only be an organization.

General Data Protection Regulation (GDPR): A set of regulations governing data protections for transferring and processing personal data from persons located in the European Union.

Health Level 7: A series of global standards for the transfer of health data between applications.

individual: A single person. An individual is interchangeable with a person. Also known as an "end user."

machine-readable: A term, a set of terms, or a completely written contract that can easily be processed by a computer.

person: A person is an individual human being. It is interchangeable with the word individual.

policy: A set of legal, political, organizational, functional, and technical obligations for communication and cooperation. (SOURCE: ISO 22600-2:2014(E) [B18])[15]

proposer: A person who advances terms and agreements to another person or entity. Proposers are the first party in their proposed contracts, and may use agents to propose terms for negotiation and eventual contract. [SOURCE: ISO 22600-2:2014(E) [B18]][16]

structured: Applies to a term or set of terms that are standardized so that they will be fixed for a context or a completely written contract, which can easily be submitted using an agent negotiated by a computer.

term: A term in this standard uses its legal meaning: a provision or condition on which a contract is based.

3.2 Acronyms and abbreviations

DPV	Data Privacy Vocabularyb
GCM	Global Compact for Migration
GDPR	General Data Protection Regulation
HL7	Health Level 7
ICT	Information and Communication Technology

[15] ©ISO. This material is from ISO 22600-2:2014 with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.
[16] ©ISO. This material is from ISO 22600-2:2014 with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.

4 Contractual agreements

4.1 Form and content

Terms for personal privacy requirements shall take the form of contractual agreements in which the person is the first party and the entity is the second party. These agreements may differ in the number and degree of protections required by persons, and in promises that might be made by both parties. There should also be as few agreements as possible, to make choosing one as easy as possible for persons and their agents as first parties, and for the agents of entities as second parties.

4.2 Location and storage

Terms and contracts shall be kept and displayed in discrete and separate forms on a public website by a neutral nonprofit entity or neutral party that is not economically dependent on terms use. These agreements shall be expressed in textual forms that can easily be understood by ordinary persons, as well as in lawyer-readable text.

4.3 Naming and labeling

Agreements shall have a consistent name, version number, and high-level description of the purposes being sought or offered in the agreement (i.e., for what purpose(s) the shared data may be used). Agreement names shall enable transparency and be meaningful when seen from the perspective of a non-specialist. These features shall make the contracts readable by humans, lawyers, and machines.

NOTE—A version number of the agreement might not be required, but only when a release date (also known as an "effective date" or "date of publication) is listed instead.[17]

4.4 Readability and formats

4.4.1 Human-readability

The human-readable component shall be a simple, easy-to-understand, and text-based explanation in plain language. This language shall specify what each party is able or not able to do with personal and related data shared under the agreement contract. Terms and contracts may use abbreviated text code and examples can be found in Annex C.

Implementors of this standard shall present contract language in the native tongue of their market of origin (e.g., English for the UK, Russian for Russia), and in any other languages as required by the market(s) they operate in or provide services for. For example, terms should be published in English and French for Canadian users (at minimum). If no such language requirements can be found in existing laws or regulator-generated rules for specific products, implementors should publish in a number of common languages that their user base is likely to speak or read on a native level (e.g., Arabic, Chinese, English, French, Portuguese, Russian, Spanish).

[17] Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this standard.

NOTE—Implementors of this standard should make agreements and contracts able to be read aloud by text-to-speech programs for individuals that are visually impaired or illiterate.

4.4.2 Machine-readability

This component shall be constructed with mechanisms enabling agreements themselves, and the individual terms within them, to be discoverable and readable by computers in a structured format. This is achieved to at least a base level by having agreements themselves recorded and published in an open and transparent online directory and having the terms within them link directly to canonical explanations and IRIs (Internationalized Resource Identifiers).

The availability of a public roster of contractual agreements (following this standard) allows those agreements to be machine readable by agents for both persons and entities, when they are in, at minimum RDF or XML formats. Example formats are located in Annex A and use JSON formats.

4.4.3 Legal readability

Agreements shall be written as formal contracts, specifying exactly what requirements, promises, and other obligations shall be obeyed by both parties, which forms the canonical agreement itself and may be read mainly by legal representatives.

4.4.4 Agreement representation formats

Agreement terms, and short codes that represent them, may have meaning to individuals and systems that understand them. An example of this kind of system may be found in Annex A.

5 Action and Interaction

5.1 How the standard works in practice

Figure 1 shows a visual representation of a sample interaction where a person, through an agent, chooses Contract_3 from a limited roster of possible agent-agreements posted by a neutral nonprofit on a public website.[18] The person's agent informs the entity's agent of their choice, and the entity's agent either agrees or declines. If the entity's agent agrees, both agents sign the agreement digitally, and both parties record the agreement in their own private data store. If the entity's agent declines to agree, the person's agent records that action in its own private data store.

[18] This same model is used by Creative Commons for licenses a person may choose for their artistic work.

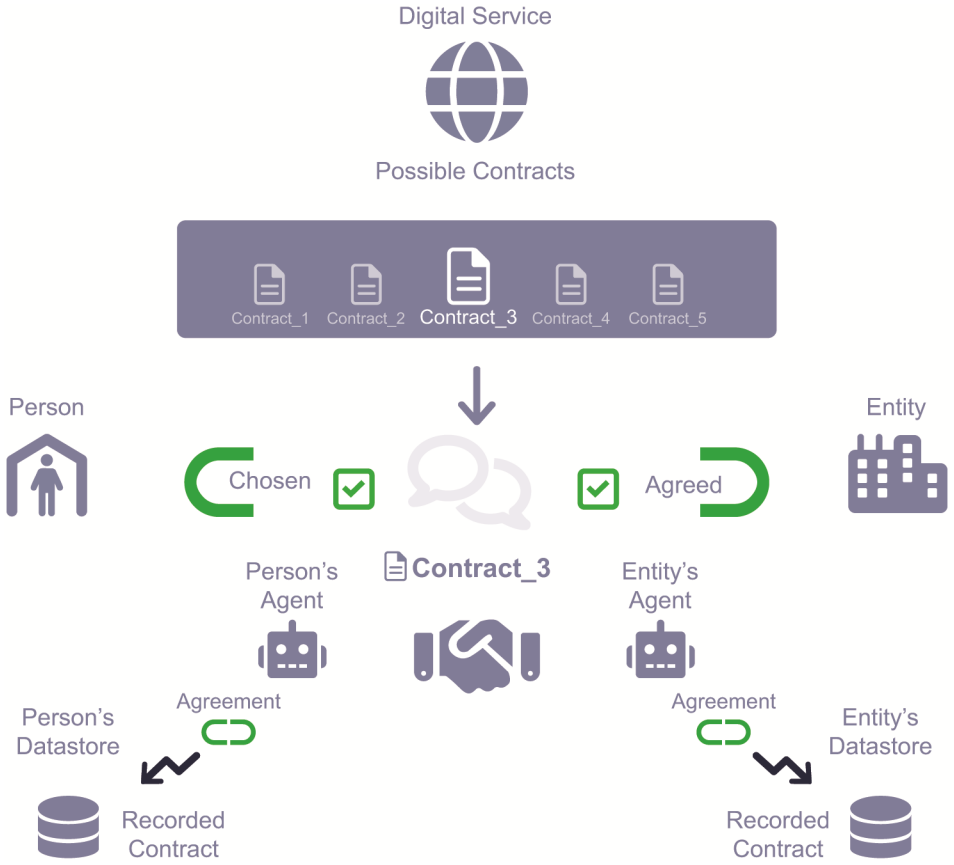


Figure 1—Sample interaction demonstrating individual presentation and entity agreement for contract completion

5.2 Agents

Agents for persons shall be any software and/or services, or a combination of software and hardware, responsible exclusively to that person. Agents for entities shall be software and/or services responsible exclusively to that entity. Agents may be provided by services external to either party but shall be controlled by, and responsible to, the represented party only.

If an agent external to one provided by the agreement-chooser selected by the person or entity is utilized (i.e., a paid agent used in a free or open-source agreement-chooser), it shall not hinder the performance of the agreement-chooser nor alter any agreement without fully educating the user about every modification made.

5.2.1 What the individual's agent does

5.2.1.1 The individual's agent

The individual's agent shall be constructed by including the components outlined in the following subclauses, with a simple interface that allows an individual to install, set up, and choose their terms. The components are organized as roles for illustrative purposes.

5.2.1.2 The chooser

The chooser is the interface a person uses to select a default agreement that shall be presented to every entity the person's agent encounters the first time or to select various agreements based on other contexts. While optionality should be maximized, the roster of possible choices should also be minimized to allow ease of use and application at scale across many entities over time.

The person's chooser interface and functionality shall be simple, allowing an individual to choose from sets of human-readable, structured agreements. Terms shall default to a locked-down state (Off) but shall be changeable by the individual, or the individual may choose to copy other settings by a known and respected individual. The individual may set their chosen terms within context as appropriate. The individual should not be asked to set many settings or make complicated choices.

These agent-agreements consisting of a short list of simple terms and agreements shall be used in contracts. Examples may be found in Annex A.

5.2.1.3 The proposer

An "under the hood" agreement proposer within an agent shall present the person's preferred agreement. It may notify the person of refusals and ask for guidance. Negotiator notifications and requests should be set globally so the person can track refusals to their terms or simply not interact with anyone who refuses without notification.

The individual's agent shall specify that the individual's chosen terms shall supersede any Terms of Use (TOU) or Privacy Policy. Examples of these licenses are located in Annex A.

5.2.2 The interaction

Agents for individuals shall be able to choose a single option from the roster of contractual agreements, to sign agreements for the person, and to put the signed agreements in a database of the person's preference. Agents for entities shall be able to agree to the person's choice of the contractual agreement and to put the signed agreements in a database of the entity's preference. Signed agreements shall be identical in both databases. There shall be no negotiation beyond the single choice by either party.

Digital copies of the signed agreements shall be delivered to both parties or their agents immediately upon agreement signing.

5.2.3 The agreement handshake

Once a personal privacy agreement has occurred and the agreement-agents representing both parties are moving forward with exchanges of data and services, the process shall notify each party that the agreement handshake is complete with a unique pseudonymous or explicit contract identifier.

5.2.4 The recorder

The contract recorder shall record the agreement and handshake terms, date, time stamp, and pseudonymous or explicit identifiers, containing a unique contract ID, and at minimum shall deliver it to both parties within a single session to the agreement-agent. The recorder shall record rejected agreements including date, time, and entity refusing the offer. The individual's agent shall have a function for submitting to anyone including auditors an agreement in dispute and shall allow the individual to explicitly

share documentation with regulators and legal representatives to review existing contracts on behalf of the individual.

5.2.5 The auditor

The auditor functions of the agreement-agent shall track sharing agreements with auditors and regulators, including the terms under which the agreement or contract is shared.

5.3 What the entity's agent does

5.3.1 The entity's framework for agreement-agent interaction

Entities shall have codes and systems that respond to individual's proffered terms. As the responding party, entities shall have the ability to:

a) Accept the terms an individual presents from the structured and bounded list

b) Respond to the individual with a single alternative set of terms from the structured and bounded list

c) Reject the proffered terms, wherein an entity cannot bar an individual from utilizing free or public information or services

Entity's signal shall go back to the individual's agent software. If an agreement is reached, entities shall collaborate with the Individual's agent to create a contract. This contract shall be signed, recorded, and deposited with the agent of both individual and entity. If an agreement is not reached, a record shall be generated to document rejection.

5.3.2 Entity Agreement System

Entities should frame their own business practices and business opportunities for their agreement systems. Entities shall develop their products and services based on full respect for personal privacy agreements to which the entities have signed. Entities shall display publicly all terms they would accept from an individual who proposes terms and agreements.

5.4 Interaction between agents

Individual agents shall propose the individual's preferred agreement to entities. When an entity's agent chooses to join in that agreement, both agents shall sign and record the agreement on behalf of each party.

5.4.1 How contracts are created

Contractual agreements shall be established once legal-layer terms have been proposed by individuals and accepted by entities in signed form.

5.4.2 How contracts are signed

Contractual agreements shall be signed electronically by both party's agents using any standard method agreed upon for that purpose.

5.4.3 Parties to contracts

There shall be only two parties to each contract. The individual shall always be the first party, and the entity shall always be the second party.

Agreements conforming to this standard shall not enable individuals to sign a single agreement instance with multiple parties under the remit of one agreement instance. Agreements shall be only between a first and second party.

5.4.4 Recording of agreements and storage

The exact time, date, and location shall be recorded in the contract and agreements. Identical, immutable copies of contracts and agreements shall be recorded in each party's data store, for possible later access, auditing, or dispute resolution.

Database storage shall include both static and dynamic pods, agents storing agreements, libraries, remote or cloud storage, local file folders on owned devices, and so forth. Storage shall be substitutable. Devices and/or services keeping databases shall be substitutable, with data portability.

5.4.5 Identities and identifiers

Contracts and agreements shall be defined between two named parties who are known to each other to the extent they need to be—both for the purpose of this standard, and to comply with existing laws and regulations.

At a minimum, all interactions in digital form include IP addresses. Named parties may include public keys, an IP address + date + epoch time, an email address, or some other pseudonymous identifier, or a combination of these elements, so long as an IP address is present. As required, an additional identifier can be applied to conform to existing laws and regulations insofar as all identifiers are appropriately labeled (e.g., IEEE 7012 Identifier, EU Regulatory Identifier).

5.5 Interoperability for ecosystems

Because the GDPR requires understanding between parties, Annex D: "Ecosystem Translation and Interoperability Principles" presents methodologies for translation and interoperability between domains without common understandings of each other for the human-readable structured agreements. Within contexts requiring translation for interoperability between disciplines without a common, simple understanding of each other (which may need to normalize the human-readable structured terms and agreements), the presented standards and systems for implementing this work should be followed.

NOTE—Interoperability between systems is not a requirement of this standard, but due to the global concern about interoperability in order to integrate new standards with existing systems, the information in the annex is provided as an optional aide to this standard.

Since implementation of interoperability between systems and domains is outside the scope of this standard, users of this standard should refer to other technical standards if the information in Annex E is insufficient to address this topic.

6. Annexes to IEEE Std 7012-2025

All annex contents are to be considered informative. Examples and samples may be utilized, and within the context of use, if following the standard, may then be required for complete implementation. However, none of these examples shall be considered normative.

What follows are examples of ways this standard can be adopted. This includes sample terms and code in Annex A, some use cases in Annex B, and ecosystem translation and interoperability information in Annex C. In Annex D, there is an Abbreviated System for Compound Terms and Agreements model for showing licensing. The bibliography is located in Annex E.

Annex A

(informative)

Draft terms with sample code[19]

A.1 Terms in draft

Overarching Principles for the sample terms that follow, and are used for implementation:

a) The individual is self-sovereign and an independent actor in the ecosystem.

b) Organizations are present in this ecosystem as voluntary providers of products and services.

c) The person provides data required for service and no more.

d) All personal data is deleted at the termination of an agreement unless expressly overridden by national regulations.

e) Any purposes and terms not overtly mentioned as allowed are not allowed.

f) Service provision utilizes an identifier for denoting the person as the recipient of that service; this method assumes the individual can bring their own; potentially supported by a software agent and related services.

g) Contractual Agreements are signed and in place before any data exchange takes place.

h) Precise data required for each purpose is out of bounds for the agreement design and selection.

i) The terms shall be drafted in a manner that facilitates the individual's decision-making by providing simplicity and convenience wherever possible, without compromising on legal protections, and without requiring the individual to read or understand large amounts of legal text.

j) The agreements and terms shall be interoperable and utilize standards-based machine-readable formats such that software agents can use this information to support the individual in making decisions and establishing agreements. For this, the agreements shall utilize relevant standards and best practices—such as the Data Privacy Vocabulary (DPV) to express purposes, data categories, and other pertinent information in an interoperable and machine-readable format, and Open Digital Rights Language (ODRL) or equivalent to express the agreement along with its permissions, prohibitions, and obligations in a standardized manner.

Based on these principles, the following terms are provided based on the existing "Creative Commons" model which uses a base term (CC-BY) that is further annotated with additional terms (e.g. CC BY-ND) to express specific permissions or restrictions. CC-BY licenses are widely utilized, are simple to express and interpret, and are backed by a robust legal framework across jurisdictions. Replicating this for IEEE Std 7012-2025, the baseline term permits only the delivery of requested/stated (SD-BASE), This is further enhanced by additional terms related to privacy or reciprocity, as shown in Table A.1. This enables the

[19] The most up to date version of these terms is located at Customer Commons through their Developer Community and can be found at http://customercommons.org/p7012/Terms

individual to easily choose their preferences from a small set of terms which are then utilized by the software agent to express corresponding agreements as a combination of the following selected terms:

A	Analytics by Second-Party
AI	AI Training and Operation
AT	Analytics and Tracking by Second-Party
ATP	Analytics, Tracking, and Profiling by Second-Party
DP	Data Portability
GOOD	Public Good
S3P	Share Anonymised Data with Third Party
PDC	Personal Data Contribution
INTENT	Intent Casting
SD	Service Delivery

Implementation of these sample terms in combination in agreements should be simple enough for the individual to understand and assert, and all terms that are not included in the agreement are expressly prohibited. Or conversely, only the terms expressly permitted in the agreement are allowed. For example, SD-BASE, as the baseline term, represents the individual's preference to receive a service without any analytics, tracking, or profiling by the 2nd or 3rd parties. If the individual wants to accept tracking and profiling by the 2nd party along with service delivery, their choice would be represented by SD BASE-AT. Table A.1 outlines the various combinations of these terms and their effects. In the table, ✓ represents the stated activity is permitted, i.e., it MAY be done, X represents the stated activity is prohibited, i.e., it MUST NOT be done, and ○ represents the stated activity is an obligation, i.e., it MUST be done.

Table A.1—Sample machine-readable privacy terms

Agreement ID	Scope	Service Delivery	Analytics 2P	Tracking 2P	Profiling 2P	Share Anonymised Data 3P	Data Portability
These (SD) agreements are relevant when the individual is receiving a service, or product that has a digital component, and thus there is an ongoing digital relationship:							
SD-BASE	Any Service	✓	X	X	X	X	○
SD-BASE-DP	Any Service	✓	X	X	X	X	✓
SD-BASE-A	Any Service	✓	✓	X	X	X	○
SD-BASE-A-DP	Any Service	✓	✓	X	X	X	✓
SD-BASE-AT	Any Service	✓	✓	✓	X	X	○
SD-BASE-AT-DP	Any Service	✓	✓	✓	X	X	✓
SD-BASE-ATP	Any Service	✓	✓	✓	✓	X	○
SD-BASE-ATP-DP	Any Service	✓	✓	✓	✓	X	✓
SD-BASE-ATP-S3P	Any Service	✓	✓	✓	✓	✓	○
SD-BASE-ATP-S3P-DP	Any Service	✓	✓	✓	✓	✓	✓
These agreements are relevant when the individual is 'providing' or 'donating' data for a specific purpose/goal, and the assumption is that these data contributions are on a one-off basis:							
PDC-INTENT	Intent Casting	✓	X	X	X	X	✓
PDC-AI	Training AI	✓	X	X	X	X	✓
PDC-GOOD	Public Good	✓	X	X	X	X	✓

✓ Required
X Not allowed
○ Optional

An example workflow for how these terms are used by software agents representing the person and the organization is depicted visually below. In the figure, the Agreement_Registry is a common, open, interoperable registry which allows different entities to refer to an agreement using unique identifiers (such as SD-BASE above) and to retrieve the terms that the agreement represents in various formats that enable software agents to use this in interactions. The person chooses their preferred terms or agreements from this registry, and their software agent (represented as Person_Agent) uses these to assess and finalize agreements with websites that the person wants to use services from.

The last three terms, PDC-INTENT, PDC-AI and PDC-GOOD should have unique contract wrappers for their utilization such as for time limited use. These contract wrappers shall not be the same as the contract wrapper for "any service" terms.

In the figure, the person chooses SD-BASE as its first choice and SD BASE-AT as its second choice for the two agreements they would be okay with. The person can have more agreements, or can also choose the context in which they apply e.g. for specific kinds of services or depending on time/location. However, for simplicity of demonstration, the figure only uses two. When the person visits the entity organization's website, its software agent (represented as Entity_Agent) must respond affirmatively to a query by the Person_Agent that it supports IEEE 7012. Then before any data or service is provided or received, the Person_Agent first asks the Entity_Agent whether it supports SD-BASE as defined in the

Agreement_Registry. If the Entity_Agent does not know this agreement, it can retrieve and analyse it from the registry. If it finds it acceptable, then the two agents have an agreement and sign the contract.

If the Entity_Agent does not accept SD-BASE, but instead it wants SD BASE-AT, it makes a counter-offer to Person_Agent asking to negotiate its chosen agreement. If the Person_Agent finds this acceptable (which it should as SD BASE-AT is an approved agreement), then it communicates the agreement and the two agents sign the contract. If the Person_Agent does not find SD BASE-AT acceptable, then it communicates this and terminates the process as IEEE 7012 does not permit more than 1 round of negotiation. Similarly, if the Person_Agent does not understand the given agreement, for example because it is not part of the common registry, it will also terminate the process. While this example was simplified for demonstration, practical usefulness of this process should be clear when considering that the organization must now state its ‘highest bid’ in terms of what is acceptable when making the counter-offer. If it had asked for SD BASE-A, it would have been accepted as its terms are a subset of SD BASE-AT which has already been approved by the individual. However, if it had asked for SD BASE-ATP, then it would not have been accepted as the Profiling (P) term is not acceptable to the individual.

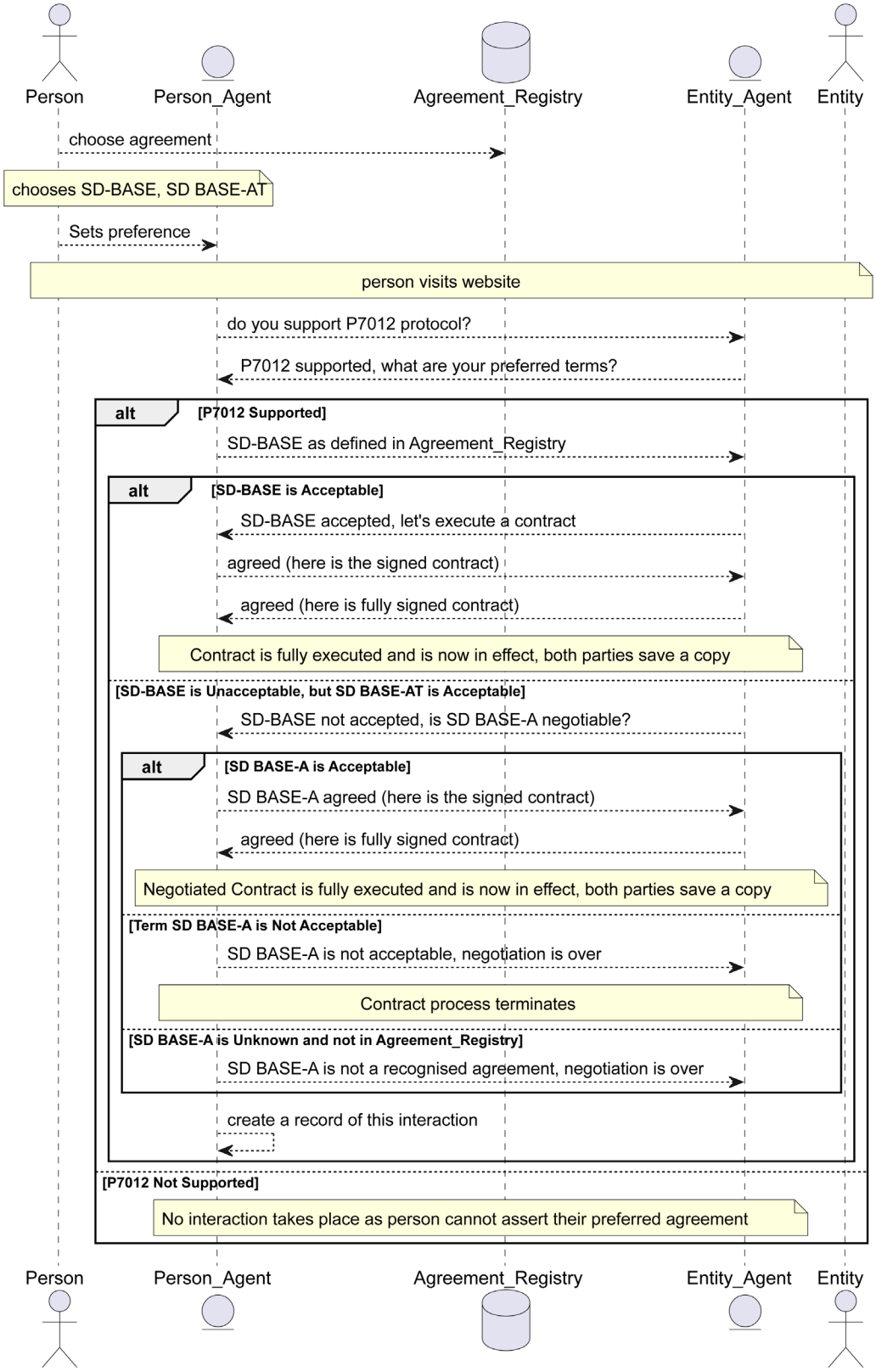


Figure A.1—Terms interaction workflow example

Further explorations of this process are not in the scope of this work. Similarly, the recording of contracts following the agreement between the two agents is also not in scope as existing efforts such as the Data Privacy Vocabulary (DPV) to express information, and Open Digital Rights Model (ODRL) to represent 'machine-readable agreements' should be used for consistency, interoperability, and establishment of common standards.

When a controlled set of agreements and agents communicate solely by selecting from these options, a more efficient form of establishing this communication is to use bitwise representation, which represents the choice of agreements within the minimum possible space. In this format, called CONTRACT ZONE, each individual privacy term is represented by a bit—where if the bit is 1 it is allowed and if it is 0 then it is not allowed. Since the minimum possible term is "Service Delivery," which is always required, it can be interpreted without an explicit representation. The rest of the terms and their bitwise representations are positioned in order as follows: Data Portability needs 1 b, Analytics/Tracking/Profiling have four states—None/A/AT/ATP and therefore need 2 b (as 00, 01, 10, 11), and Third-Party anonymized data sharing needs 1 b. This means a string "0000" represents Data Portability not required, and nothing else is allowed; whereas a string of "1100" represents Data Portability is required (1st digit is 1), and Analytics and Tracking are allowed (2nd and 3rd digit are 10 and represent AT), and third-party sharing is not allowed. The remaining purposes of Intent Casting, AI Training, and Public Good will require a further 1 b each to represent whether they are applicable or not. The entire string is thus at a maximum length of 6 b, and two letters in hexadecimal with space for future expansion.

A Machine-Readable Personal Privacy Agreement proffered by individuals provides privacy terms that can be read and agreed to by networked machines on behalf of entities. Traditional passports have used Optical Character Recognition (OCR), which uses ISO/IEC standard formats for machine operability. Similarly, Machine Readable Privacy Terms should be in a universally readable format. Table A.2 suggests encoding/interpreting two lines that collate machine-readable privacy agreements made of Boolean choice operators providing a simplistic standard layout for privacy agreements. This two-line agreement adheres to a pre-arranged format, with a specified character limit and length.

The machine-readable encoding process allows for the standardization of a proffered agreement that can be translated into another domain language/process without the need for complex translation methodologies. These limitations would be like the format of the machine-readable zone on machine-readable passports that allow for interoperability between autonomous processing systems.

Table A.2—Sample code for expressing terms

Individual proffered terms information hierarchy	
Value	**Entry**
(v) 0.1 Terms	
(t) 0.1 Generic	
Language	
++++++++++	Proviso
ROW-1++++++	Term (1 – SD-BASE)
(r) English (USA)	Service Delivery
Vocabulary	https://w3id.org/dpv/standards/p7012 # ServiceDelivery
Canonical URL	https://.../agreement/ sd-by/0.1/
Human-Readable	https://.../agreement/sd-by /0.1/human.en
Machine-Readable	https://.../agreement/sd-by /0.1/machine.en.rdf/xml/rss
Legal-Readable	https://.../agreement/sd-by /0.1/legal.en
ROW-2++++++	Term (AT)
(r) English (USA)	Analytics and Tracking by SecondParty
Vocabulary	{{CONTINUE AGREEMENT FORMAT}}

The construction of the agreements into machine-readable privacy states reflect both standard OCR formats of travel documentation. The concept of travel documents has been through generations of protocol and scrutiny. Combined with analog standards (such as machine-readable passports (MRP) which are machine-readable travel document that follow Document 9303 by the ICAO) [B14] for travel documents, agreements and contracts provide an example for generating machine-readable agreements. Basing machine-readable privacy agreements on traditional non-digital or analog systems allows for the adoption of these techniques to systems that can be easily emulated within digital environments.

A.2 HTTP request example

As the digital privacy landscape continues to evolve, there needs to be a simple way to send and receive privacy-based **CONTRACT** requests with other endpoints on the internet. One approach to this is to structure the request in an HTTP header which can simplify process and compliance. Below is an example of the machine-readable privacy **CONTRACT ZONE** of the HTTP header request when starting a new Windowed Session.

```
GET /network-resource HTTP/1.*
Host: Yahoo.com
MRPAZ-A: org.CuCo
```

```
MRPAZ-V: V0.1
MRPAZ-T: GEN
MRPAZ-R: USA
MTPAZ-1: BSD2SIA2ETI2CPE2
MTPAZ-2: CNT2CIT2CPT2CSD2
MTPAZ-3: 38
```

Once the handshake is accepted and the **INDIVIDUAL(s)** terms are proffered, a checksum number can be shared to lower the overhead of the signal transmission.

HTTP request example description:

- `GET /network-resource HTTP/1.*` this specifies the standard method, path, and HTTP version being used.
- `Host: [Yahoo.com](<http://Yahoo.com>)` This specifies the top-level domain address of the end-point sever.
- `MRPAZ-A: org.CuCo` this the namespace/ authority code being used to proffer the CONTRACT context.
- `MRPAZ-V: V0.1` This is the version control number of the privacy CONTRACT toolset being used.
- `MRPAZ-T: GEN` This is the type of privacy CONTRACT toolset being used.
- `MRPAZ-R: USA` this is the regional legal framework being used for the privacy CONTRACT
- `MTPAZ-1: BSD2-SIA2-ETI2-CPE2` This is the first row of the Machine-Readable Privacy CONTRACT and represents SD BASE-ATP-S3P (as hex 38 = 0111000) .
- `MTPAZ-2: CNT2-CIT2-CPT2-CSD2` This is the second row of the Machine-readable Privacy CONTRACT.
- `MTPAZ-3: I1` This is the intentcasting row where T1 is an example of an intent scenario definition.

A.3 RDF/Turtle

```
@prefix dcterms: <http://purl.org/dc/terms/>
@prefix odrl: <http://www.w3.org/ns/odrl/2/>
@prefix p7012: <https://w3id.org/dpv/standards/p7012#>
@prefix dpv: <https://w3id.org/dpv#>
@prefix xsd: <http://www.w3.org/2001/XMLSchema#>

<http://example.org/SD-BASE-AT> a odrl:Offer ;
   odrl:uid <http://example.org/SD-BASE-AT> ;
   odrl:profile <https://w3id.org/dpv/mappings/odrl> ;
   dcterms:title "SD BASE-AT";
   odrl:conflict odrl:perm ;
   odrl:permission [
      odrl:action p7012:Analytics2PAllowed,
                              p7012:Tracking2PAllowed ;
      odrl:assignee p7012:Entity ;
   ] ;
   odrl:obligation [
```

```
    odrl:action p7012:ServiceDeliveryRequired ;
    odrl:assignee p7012:Entity ;
] ;
odrl:prohibition [
    odrl:action p7012:ProfilingDisallowed,
                            p7012:DataSharingDisallowed ;
    odrl:assignee p7012:Entity, p7012:ThirdParty ;
] ;
odrl:prohibition [
    odrl:action p7012:Analytics3PDisallowed,
                            p7012:Tracking3PDisallowed ;
    odrl:assignee p7012:ThirdParty ;
] .
```

A.4 JSON

```
[
{
  "   ServiceDelivery": {
   "purpose": "   ServiceDelivery",
   "condition": "on"
  }
},
{
  "   Analytics": {
   "purpose": "   AnalyticsOfServiceUsage",
   "condition": "on"
  }
}
]
```

A.5 JSON-LD

```
{
  "@context": {
    "skos": "http://www.w3.org/2004/02/skos/core#",
    "dpv": "https://w3id.org/dpv#",
    "p7012": "https://w3id.org/dpv/standards/p7012#",
    "rdfs": "http://www.w3.org/2000/01/rdf-schema#",
    "dct": "http://purl.org/dc/terms/"
  },
  "@id": "p7012:SD-BASE-AT",
  "@type": ["p7012:Agreement", "rdfs:Class", "skos:Concept"],
  "skos:broader": {"@id": "p7012:SD-BASE-A" },
  "skos:definition": "Term that requires Service Delivery, and
permits Analytics and Tracking by the 2nd Party, and prohibits
Analytics, or Tracking by 3rd Party, prohibits Profiling by 2nd and
3rd Party, and prohibits sharing any data with 3rd Party",
  "skos:prefLabel": {"@id": "SD BASE-AT" },
  "dpv:hasObligation": {"@id": "p7012:ServiceDeliveryRequired" },
  "dpv:hasPermission": [{ "@id": "p7012:Analytics2PAllowed" },
    { "@id": "p7012:Tracking2PAllowed" }],
  "dpv:hasProhibition": [{ "@id": "p7012:ProfilingDisallowed" },
    { "@id": "p7012:Analytics3PDisallowed" },
    { "@id": "p7012:DataSharingDisallowed" },
    { "@id": "p7012:Tracking3PDisallowed" }],
```

```
  "p7012:hasHumanReadableFormat":
      "https://example.com/human/SD-BASE-AT",
  "p7012:hasMachineReadableFormat": {
    "dct:conformsTo": "https://www.w3.org/TR/odrl-vocab/",
    "dct:identifier": "https://example.com/ODRL/SD-BASE-AT"
  }
}
```

A.6 RSS

```
<?xml version="1.0" encoding="utf-8" ?>
<rss version="2.0">
<contract>
  <title>Privacy CONTRACT via RSS</title>
  <description>This is an example of serving a Privacy CONTRACT
               via RSS</description>

  <link>https://.../agreements/</link>
  <lastBuildDate>7 Oct 2024 18:22:02 +0000</lastBuildDate>
  <pubDate>4 Jun 2024 18:22:02 +0000</pubDate>
  <ttl>1800</ttl>
  <agreement>
   <title>   ServiceDelivery</title>
   <purpose>   Service Delivery Agreement</purpose>
   <token>BSD</token>
   <state>2</state>
   <link>https://.../agreement/   sd-by/0.1/</link>
   <pubDate>4 Jun 2024 18:22:02 +0000</pubDate>
  </agreement>
</contract>
</rss>
```

A.7 PKL (Pickle)

In this example, CONTRACT is defined using PKL (Pickle), which can generate JSON, YAML, PROPERTY LISTS, and many other formats.

```
name = "BasicServiceDelivery"

agreement {
  namespace = "CuCo"
  purpose = "   Service Delivery Agreement"
  token = "SD BASE-ATP   "
  state = 2
}
```

A.8 JSON via Pickle

```
{
  "name": "   ServiceDelivery",
  "agreement": {
    "namespace": "CuCo",
    "purpose": "   Service Delivery Agreement",
    "token": "   SD BASE-ATP",
```

```
    "state": 2
  }
}
```

A.9 YAML via Pickle

```
name:    ServiceDelivery
agreement:
  namespace: CuCo
  purpose:    Service Delivery Agreement
  token:    SD BASE-ATP
  state: 2
```

A.10 PLIST via Pickle

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
   "http://www.apple.com/DTDs/PropertyList-1.0.dtd">

<plist version="1.0">
<dict>
  <key>name</key>
  <string>   ServiceDelivery</string>
  <key>agreement</key>
  <dict>
    <key>namespace</key>
    <key>purpose</key>
    <string>    Service Delivery Agreement</string>
    <key>token</key>
    <string>   SD BASE-ATP</string>
    <key>status</key>
    <integer>2</integer>
  </dict>
</dict>
</plist>
```

A.11 PROPERTIES via Pickle

```
name =    ServiceDelivery
agreement.namespace = CuCo
agreement.purpose =    Service Delivery Agreement
agreement.token =    SD BASE-ATP
agreement.state = 2
```

Annex B

(informative)

Use cases

These two use cases are in the style of stories that would typically be given to an engineer as an overview of how the standard will work. The purpose is to have engineering connect personally with the individuals using the products and services.

The following use cases are included as references: 1) No stalking (written in the style of usability) and 2) Intentcasting (written in the narrative style).

B.1 Use Case 1: No stalking

This use case uses a standard usability template developed from Craig Larman book, Writing Effective Use Cases (Larman, Chapter 6 [B29], Cockburn [B4]). A use case was developed previously in the Kantara / Customer Commons User Submitted Terms Working Group and was titled: No Stalking. The idea was to address the advertising tracking and collecting of data as individuals (end users) would interact with products and services via the web or apps. For Exemplary Human- and Legal-readable layers, see "User Submitted Term—UX and Interface V.2: "No Stalking" Term [B36].

INDIVIDUAL STORY: A news reader of many different news sites is a non-subscriber and wants to read a news site without being tracked, but still allowing ads to be shown.

PURPOSE: To address the individual's distaste for services and systems that track and collect data, the person (an end user) should have more control over the terms, and their data as shared through their agent and under the contract between two parties.

GOAL: The individual has the means to read (human-readable), contract (legal-readable), and present (machine-readable) terms to websites and applications via a user-agent. Individuals can pay as much or as little attention to the terms presented once they have chosen to invoke terms. Individuals might defer their terms selections to other trusted individuals and experts and may decide to ignore negative responses, or simply navigate to alternative products and services compatible with the terms the individual has selected.

ACTOR 1: End user or Individual who uses a website or app

ACTOR 2: Entity responsible for agreements and terms for websites or app products and services

PRECONDITION: Services and products exist, and are discoverable by the individual, and compatible with the individual's device(s) and user agent(s) (browsers or application system/host). A given service or product would utilize code to receive terms from the individual's agent and agree or respond with a suggested alternative within structured terms. Websites are composed of more than the 2nd party entity. These include any 1st, 3rd, and *n*th party entities, that are benign but who may embed tracking and aggregation tools into 2nd party services, features from other nth entities, and so forth. That can be used to aggregate and track individuals. Schemas and sample code in agents distinguish on behalf of the individual between benign 3rd parties and others that may be banned from their normal functions in the 2nd party environment.

OLD WORLD SCENARIO: The individual navigates to a website. The site is already prepared for visitors with a standing Terms of Use and Privacy Policy. The site has the ability to understand and respond to terms submitted by the individual's agent. Individual's agent presents terms to the site. The site responds

with answers and possible modifications to their TOU / PP defaults. Next, the individual is presented with a signal that states the site has accepted terms and they can be found in the agent folder. Individuals proceed with their goal of accessing information on the site, knowing that their terms have been accepted and their data will be respected by the site.

NEW WORLD SCENARIO: The individual navigates to a website and the agent proffers terms. The entity has the ability to understand and respond to terms submitted by the individual's agent. If the entity rejects the single offer, the individual's agent records the rejection in their data store. If the entity accepts the offer, the agent works with the entity's agent to sign and record the immutable copy of the contract. Contracts can be found in the agent folder.

DRAFT SCENARIO II: Individual selects an app for download and installation on their device. In using the app, the app maker uses a wrap around web services pages that load from a server. The site is already prepared for visitors with a standing Policy. The individual utilizes another service app or the main operating system, which acts as the user's agent to present and negotiate terms. The site also has the ability to understand and respond to terms submitted by the individual's agent. The individual's agent presents terms to the app maker. App maker responds with an alternative structured term, which would supersede their TOU/PP defaults. The individual is presented with a signal that states the site has accepted the terms and the recorded contract can be found in the agent's folder. Individuals proceed with their goal to access information on the site, knowing that their terms have been accepted and their data will be respected by the site.

ALTERNATIVE PATHS:

a) The individual's agent presents terms to a website or app, but the site is not prepared to answer, nor does it understand the terms in a machine-readable way. The individual is presented with a signal from their agent alerting them to the lack of response. Individuals may decide to navigate to a different site that may understand and accept the terms. The agent may present the individual with alternatives more amenable to the individual's terms. Individuals may decide to use the site anyway.

b) The individual's agent presents terms to a website or app, but the site rejects some or all of the terms. The individual is presented with a signal from their agent alerting them to the rejection. Individuals may decide to navigate to a different app or site that may understand and accept the terms. The agent may present the individual with alternatives more amenable to the individual's terms. Individuals may decide to use the app or site anyway.

c) Individuals may decide to set the agent to reject any app or site that does not accept terms and navigate to sites that would accept terms as substitutions.

d) Individuals may decide to set the agent to allow the use of certain favored apps or sites that do not accept terms but which the individual wants to use regularly, without anything more than a small signal regarding lack of compatibility.

e) Individuals may decide to set agents to follow other trusted user or entity settings to defer responsibility for understanding the implications of their term choices. This choice would enable individuals to allow others who are perceived as experts to lead privacy and data control choices for community members.

f) Apps or Sites whose acceptance of terms at one point in time would likely need to update these contracts over time, for new data shared over time, if the contract no longer applies.

g) Apps may participate in a marketplace that already understands terms and has APIs for signaling responses.

POSTCONDITIONS: The individual should have access within their agent to records showing their terms, contracts, sites, and answers to their presented terms, as well as changes to terms and other information about agreements made over time.

Use Case: No Stalking Interaction Work Flow

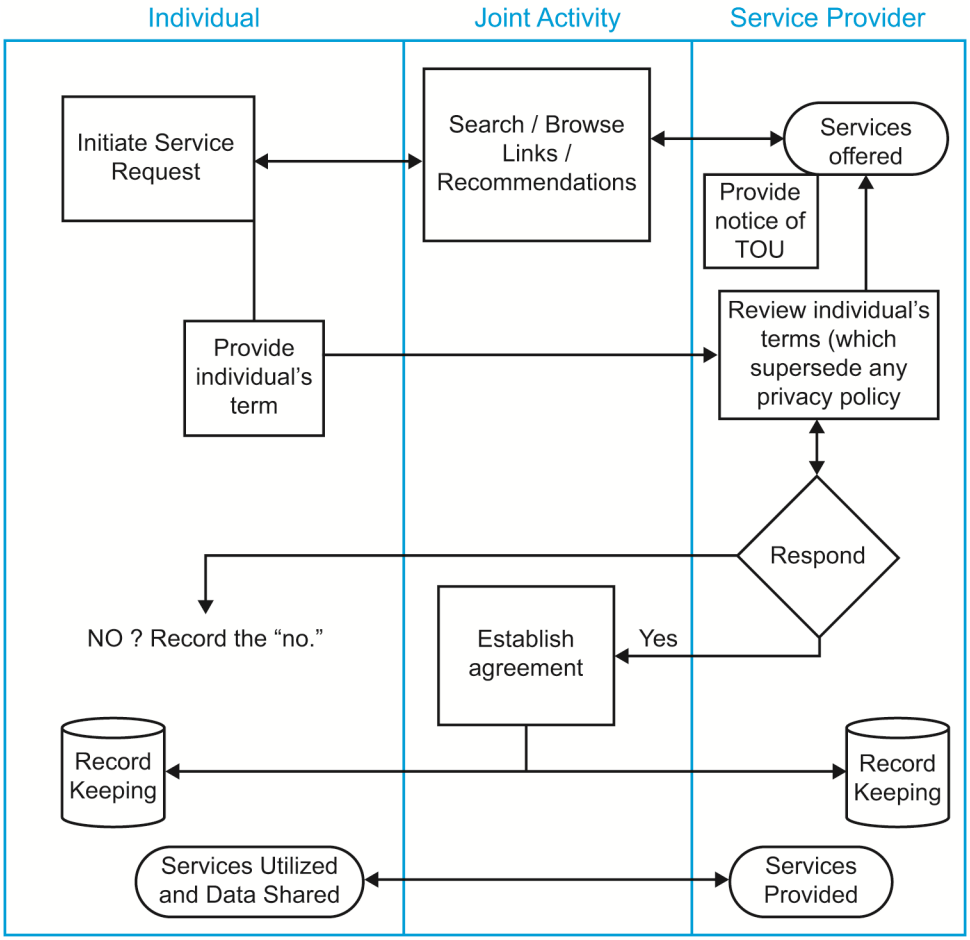


Figure B.1—Use case: No stalking interaction workflow

B.2 Use Case 2: Sharing personal buying interest data (aka intentcasting or broadcast shopping)

(Narrative format) When an individual is in the market for a product or service, they inevitably share data. This applies in the real world, but much more commonly now in the digital realm.

At present the terms under which buying interest-related data are shared are defined by the seller/ provider of products or services; or intermediaries who are incentivized to gather and use that data for their benefit (even if also benefiting the buyer and seller through their facilitation.

When the seller/provider sets the terms and provides no or very limited choices, then the individual is typically forced into sharing more than they may ideally wish to. But as the individual is actively seeking to buy or engage with a product or service; they would rarely step away from the proposed terms as that would lessen their options.

This standard allows the building and use of agreements that offer an alternate mode. In the new model, the scenario would differ. In the target mode, the individual has one or more agreements in which the terms around data exchange are transparent. That transparency should include terms and agreements that are enabling practices that the individual would likely object to if they a) could easily see those terms in advance of data exchange, and b) had the option to point to alternate agreements.

The following is an illustration of how that would work in practice. Alice is looking at options for a weekend city break with her partner James. She normally uses *WebSiteXYZ* when researching such in-town breaks, but has noticed over time that no sooner has she kicked off some basic searches for options than she gets bombarded with adverts and marketing messages both from *WebSiteXYZ* and also other advertisers she does not recognize.

See example machine-readable terms and data schema that can help enable the supply side to understand, consume, and respond to the data proffered by the individual in footnotes.[20]

INDIVIDUAL STORY:

One of Alice's friends, Megan, had mentioned she'd had a good experience with *WebSiteABC*. Alice decides to have a look at that service. The first thing she notices is the unusual 'cookie banner' which says 'We do not track personal information unless you opt into one of the standard information sharing agreements that we accept that allows this when you sign up for an account.

Alice likes the sound of that model and decides to try *WebSiteABC* for her trip research and potentially booking through the site. Her research on trip options goes well and she decides to book her trip through *WebSiteABC*. Doing so means setting up a customer account with them. She is pleased to see that very early in the account set-up process she is told that she can select from a range of 10 standard agreements to use that cover what data she would share with *WebSiteABC*, and for what purpose. Those agreements are hosted at a disinterested third-party non-profit.[21] Each has a straightforward description that explains the differences between the various agreements and offers some guidance via a Chooser/Wizard to help her find the right one given her preferences and the nature of the product and service she is engaging with. For example, the agreement she may choose for trip booking may differ from those around researching a medical condition. All of the agreements available at the third-party non-profit are designed, from the perspective of the individual/ buyer, to exclude some of the more dubious data sharing practices in the current model, like third-party sharing and tracking across the web, beyond the site in use.

Alice goes through the agreement-chooser process and concludes that agreement 4b (name and short description to be confirmed) from the Customer Commons List. This is one of the agreements that *WebSiteABC* has confirmed in advance that they accept. It allows them the following purposes to be associated with the data that Alice would be sharing under that agreement:

- Service delivery (enabling trips to be booked and taken)
- Service Improvement Analytics
- Entity tracking of individuals (on-site/in-app)
- Correlation and profile building allowed of the individual by legal entity
- Data portability, to return a copy of the data that individual shares and generates to be returned to her

Each of these allowed purposes has a very precise and easy-to-understand explanation in the agreement that both Alice and WebSiteABC sign the contract. The agreement has additional machine-readable and lawyer-oriented versions.

[20] Sample terms may be found at https://customercommons.org/choose-myterms/#IEEE-p7012-init.
[21] Ibid, 20.

Annex C

(informative)

An abbreviated system for compound terms and agreements

An abbreviated system for displaying and recognizing agreements with specific terms may be developed as the following example shown here, as modeled after a prior methodology. This information is given for the convenience of users of this standard and does not constitute an endorsement by IEEE of these products. Equivalent products may be used if they can be shown to lead to the same results: https://customercommons.org/p7012/abbreviated-designations

Annex D

(informative)

Ecosystem translation and interoperability principles

The project of defining and representing "machine-readable personal privacy terms" determines and controls the intended behavior of smart business systems and their involved actors. Implementable components of such systems may be represented using highly expressive, context-free languages such as programming languages. The intentions of the business systems' actors from different domains, using different methodologies, languages, and representation styles, based on different education and experiences, are strongly context-dependent. Therefore, the development of machine-readable personal privacy terms relies on the formal representation of the related business systems from the perspectives of the different actors and their use-case-specific mapping/harmonization. The following Annex D section defines and describes the formal representation of systems, the formal representation of multiple policies ruling the behavior of the business systems in consideration, and the related business processes, as well as the mechanisms for mapping the representations for each use case.

D.1 Background

Interoperability happens when two or more actors as part of a business ecosystem communicate and collaborate – or interact – to achieve a common goal. Therefore, interoperability requirements define the aspect and quality of interactions needed to achieve the aforementioned business objectives. In other words, interoperability is mediated by the common interactions performed. The actors involved can be any type of principal (person, organization, device, application, component, or single object).

Interoperability is defined by IEEE as the "ability of two or more systems or components to exchange information and to use the information that has been exchanged" (IEEE Std 610-1990 [B15]). The interoperability specification has evolved over the last 25 years from structured messaging (e.g., EDI, HL7 messaging) through sharing concepts (e.g., openEHR Archetypes, EN/ISO 13940 ContSys concepts)—both representing the data/information exchange paradigm—to cooperation at the application level of service sharing (e.g., web services). Nevertheless, all those standards-based interoperability approaches are restricted to computer-to-computer communication, representing information following ICT ontologies specified in the domain-independent ISO/IEC 10746 Information Technology—Open Distributed Processing—Reference Model or by domain-specific information models such as ISO/HL7 21731 Health informatics—HL7 Version 3—Reference Information Model. Meeting the objectives of improving the trustworthiness, safety, quality, and efficiency of business processes with information and communication technology support requires advancing interoperability between computer systems towards a business process-specific cooperation of actors representing the different domains participating in the business case and sharing their specific knowledge.

System theory and system engineering provide methodologies to describe the structure and behavior of any system from technical through living, organizational to even social systems, thus supporting multidisciplinary approaches. A system's structure and behavior regarding its components, their functions, and interrelations is commonly called a system's *architecture*. In other words, the structural and behavioral aspects of a system are described by its architectural model. Comparable systems follow the same architectural reference, also called an architectural framework or reference architecture. Depending on the scale of a system design, i.e., the definition of the system's boundaries, components of the system environment can be integrated into the system of consideration (internalization) or moved from the system to its environment (externalization). This process results in any level of complexity from elementary particle to the universe, or from a single gene to an entire population.

D.2 The rationale behind the approach

It is impossible to represent a highly complex, highly dynamic, multi-disciplinary/multi-domain ecosystem by one domain's terminology/ontology or by using ICT ontologies. For different reasons—including the complexity challenge—ICT standards and specifications developed within one domain (e.g., physics, chemistry, biology, legal affairs) cannot fully and consistently represent the complete background knowledge, any conceivable instance in any conceivable context of that domain and its relations to other domains. Therefore, it is impossible to justify the correct, complete, and consistent integration of, and interoperability between, independently developed systems across different domains from the ICT perspective expressed in quite simple ICT ontologies. The same holds of course for specifications independently developed within a multi-disciplinary area such as healthcare. The integration of, and interoperability between, ICT subsystems (e.g., specifications, implementations) to analyze, design, or run a multi-domain business system *is* be guided by concepts, conditions, and contexts of that real-world business system. The formal representation and harmonization of knowledge spaces and compositions, as well as policies guiding the behavior of the involved domain-specific subsystems and their relations, allow correct modeling integration and interoperability. For this reason, the agreed domains' knowledge—including individual and environmental contexts (e.g., language, education, skills, experiences, social and psychological aspects)—will be represented correctly and formally for integration into the ICT system as part of the business ecosystem; so enabling correct and consistent systems integration and domain knowledge-based interoperability.

D.3 The ISO 23903 Interoperability and integration reference architecture

ISO/IEC 10746 provides an enterprise architecture framework for the specification of open distributed processing (ODP) systems, consisting of five viewpoints expressed in ICT ontologies. It supports distribution, interworking, portability, and platform and technology independence. It complies with established software development approaches such as the Rational Unified Process. However, there is a particular shortcoming with ISO/IEC 10746. When domain experts describe specific aspects of their business ecosystem in a specific context, using their specific terminologies and ontologies, methodologies, and frameworks, the resulting informational representations are quite inconsistent, requiring a peer-to-peer interoperability adaptation process. Adapting existing standardized informational representations of domain-specific use cases to changing contexts or including other domains requires another common harmonized informational representation, resulting in permanent revisions of specifications.

ISO 23903, however, supports cross-domain cooperation of actors involved by knowledge sharing at the domain level and even in individual contexts, so establishing advanced interoperability. Thus, ISO 23903 extends ISO/IEC 10746 by a real-world business system viewpoint representing the different domains contributing to the use case by those domains' ontologies (Figure D.3).

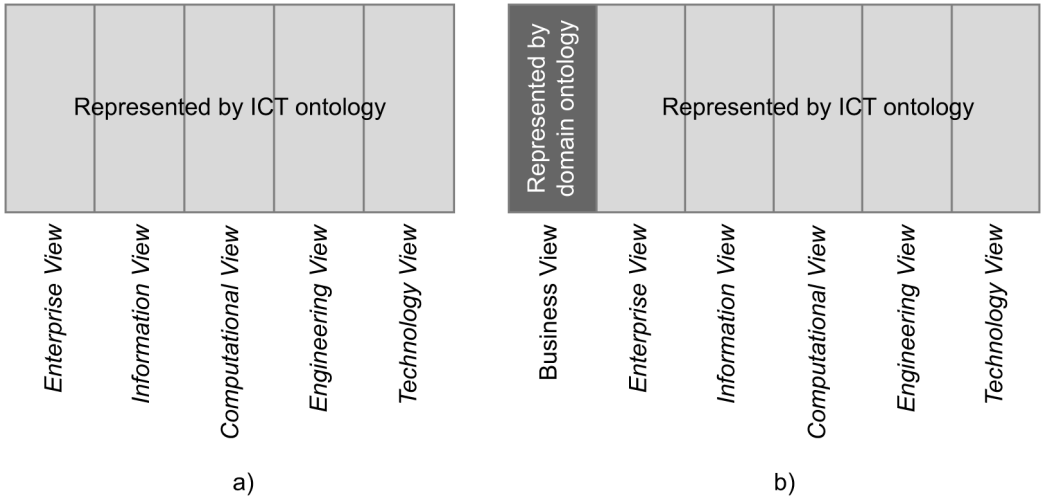


Figure D.1—Views on Ecosystems in their development process

The added Business View in Figure D.1 b) is intended to model the real-world system of all stakeholders involved in the particular type of business ecosystem, including their privacy preferences. (Note that this view may model a specific business or a type of business.) For managing the multi-disciplinary concept space, the standard introduces a generic system architecture represented through top-level ontologies, which is a use case specifically instantiated by ontologies of the domains contributing to the business case. The approach combines universal type theory and corresponding logic represented through a parameterized Barendregt Cube (see Kamareddine, Laan, and Nederpelt [B26]) with systems theory to manage the uncertainty of highly complex and highly dynamic systems as they happen, e.g., in 5P medicine (see Pires, et. al [B31]) (Figure D.2). This may represent any system architecturally (i.e., the system's components, their functions, and internal as well as external relations) by generically describing its composition/decomposition as well as the aspects (domains) of the system relevant in a specific context (e.g., business case) at a reasonable level of granularity.

To model the concepts and relations of the domain-specific subsystems involved in the business case formally and correctly, those subsystems are represented by their corresponding approved domain ontologies, resulting in a system-theoretical, architecture-centric, ontology-driven approach. The reference architecture model may be used recursively, representing, for example, the real-world systems' continuum from elementary particles to the universe, thereby overcoming the aforementioned complexity challenge. By further combining this model (introduced in the 1990s as Generic Component Model—GCM) with ISO/IEC 10746's Open distributed processing—Reference model as well as incorporating the applicable real-world rules and constraints, the ISO 23903 interoperability and integration reference architecture model and framework is complete (Figure D.2). Thus, ISO/IEC 10746 is not just extended by an additional viewpoint, but also transformed into a multi-domain schema.

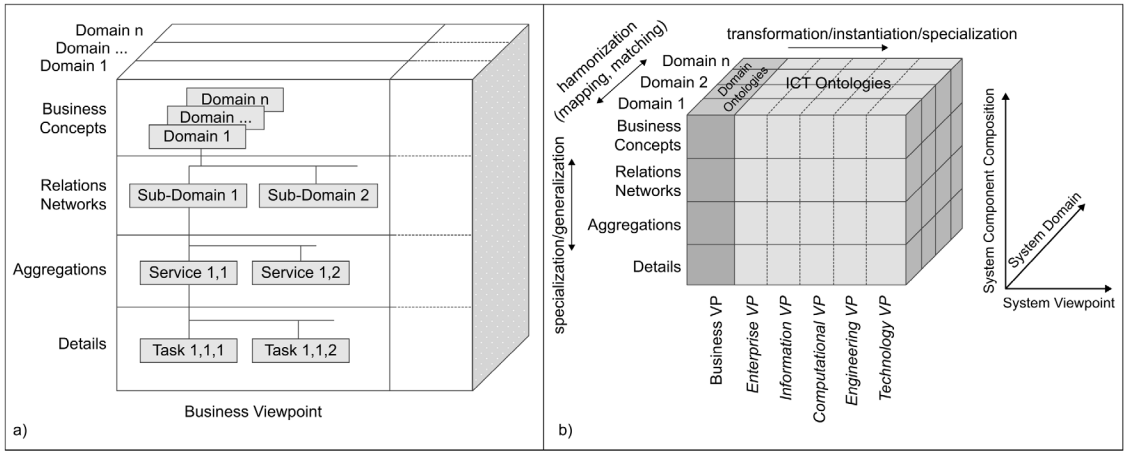


Figure D.2—According to the ISO 23903:2021 Interoperability and Integration Reference Architecture—Model and Framework

The resultant interoperability and integration reference architecture (IIRA) model allows the consistent transformation and interrelation of any domain-specific subsystem's structure and behavior (including domain-specific standards and specifications) by ontologically representing concepts and relationships at the real-world system component's level of granularity. In other words, the domain-specific subsystem (e.g., a domain-specific standard or specification) is re-engineered using the IIRA Model, by that way providing a standardized interface to that specification without the need to revise that spec (Figure D.3).

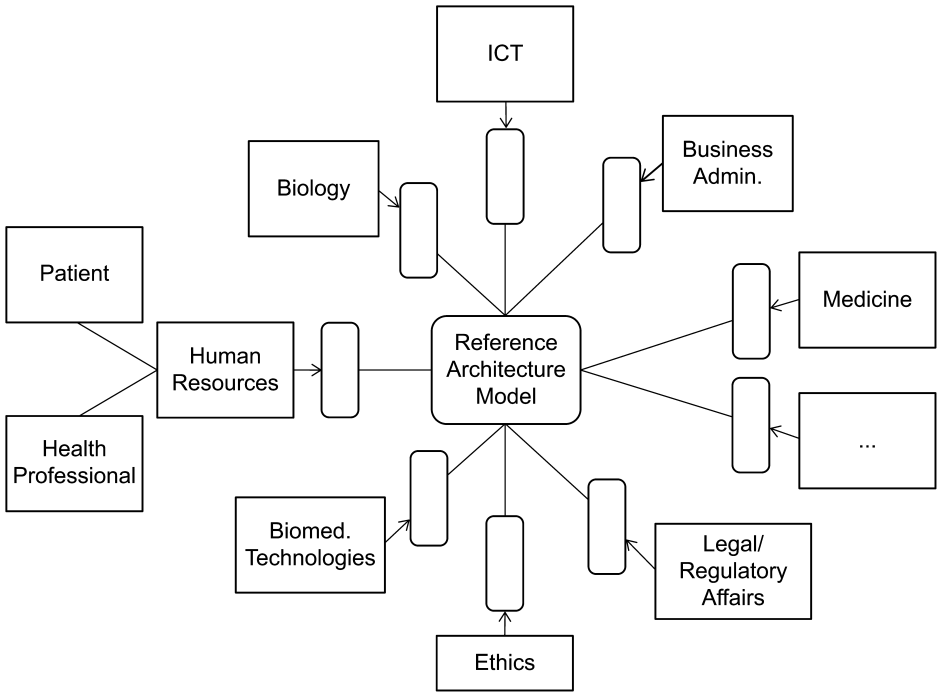


Figure D.3—The ISO 23903:2021 interoperability and integration approach exemplified for the healthcare domain

ISO 23903 defines a system-oriented, ontology-based, policy-driven, sustainable model and framework for managing systems integration and advanced interoperability across multiple domains. It enables the analysis and design of multi-domain systems, and also systems integration by the use-case-specific deployment of existing standards and/or artifacts from different domains, i.e., selection, placement, and constraining of the ICT components and their relationships. Contrary to traditional enterprise architectures, ISO 23903 provides a way to easily reconcile different knowledge domains without requiring the alteration of their inherent structures and semantics to fit each other as well as the ICT domain. This implies the reconciliation of perspectives and requirements of the domains' stakeholders without bothering them with technology.

The ISO 23903 interoperability and integration reference architecture plays the same role for domain knowledge-level interoperability as EDI and the HL7 Communication Standard did for data and information level interoperability.

ISO/IEC CD 21838 is used to support knowledge representation of the different domains involved in the business system, as well as the harmonization for mapping and matching concepts across networks of information systems.

D.4 The deployment of ISO 23903 in the IEEE 7012 context

Bound to the Global Compact for Migration framework (GCM) [B10], inter-domain relationships must happen at the same level of granularity (EN/ISO 13940:2016 [B8]). To get there, intra-domain specializations/generalizations may be performed. In summary, the interoperability reference architecture model and framework support ontology harmonization or knowledge harmonization that enables interoperability between existing systems, standards, and solutions of any level of complexity without the demand for continuously adapting/revising those specifications. Figure D.4 exemplifies the interoperability reference architecture for an instance of a generic business use case related to this standard for machine-readable personal privacy terms.

"Machine Readable Personal Privacy Terms" represent the policy contracted between the service user (Individual) and service provider, expressed as a dynamic business use case policy (see Personal Policy Domain in Figure 4b of ISO 22600-2:2014 [B18]). A system's policy describes the rule sets controlling the behavior of the business ecosystem for a specific use case by constraining the system's components, their functions, and relations. The use case policy domain is a composition of many policy subdomains such as the service user policy representing an individual's wishes and expectations, the contextual policy, the legal policy, and the service provider policy. The contextual policy may be specialized in environmental and conditional policies (health status, occupational issues, social implications, and so forth), impacting the service provision and consumption over time.

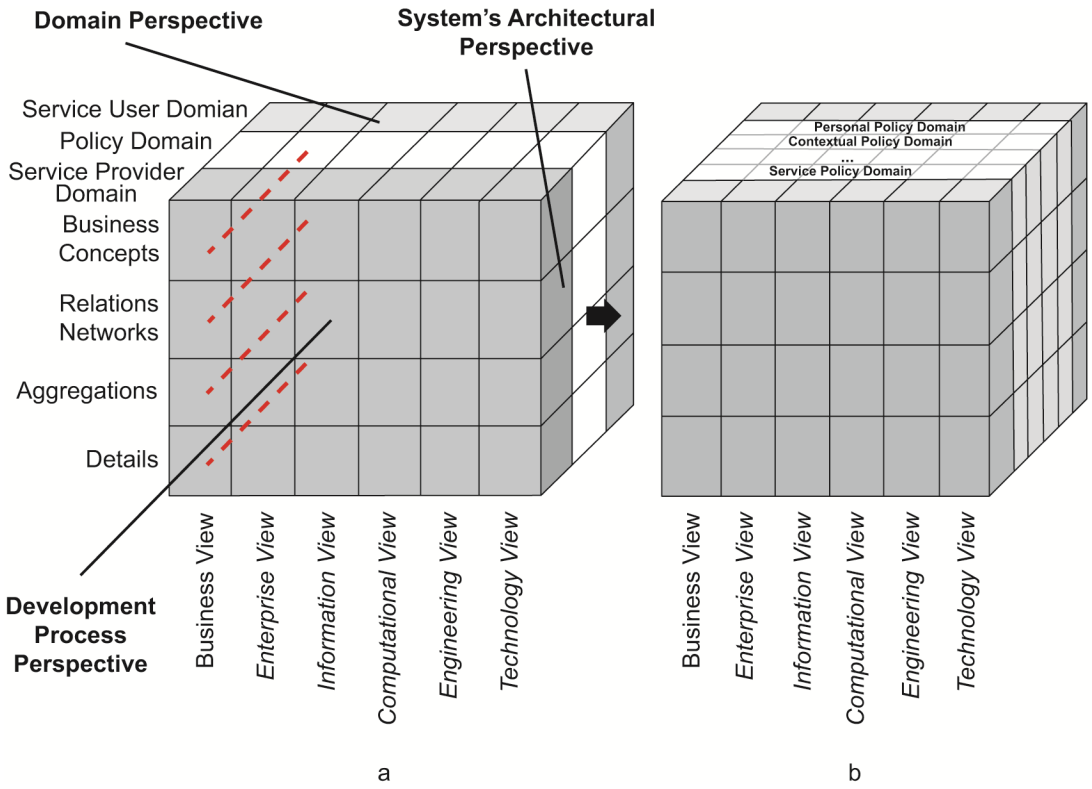


Figure D.4—Specialization of policy domains according to ISO 23903:2021 modified with this standard concepts applied

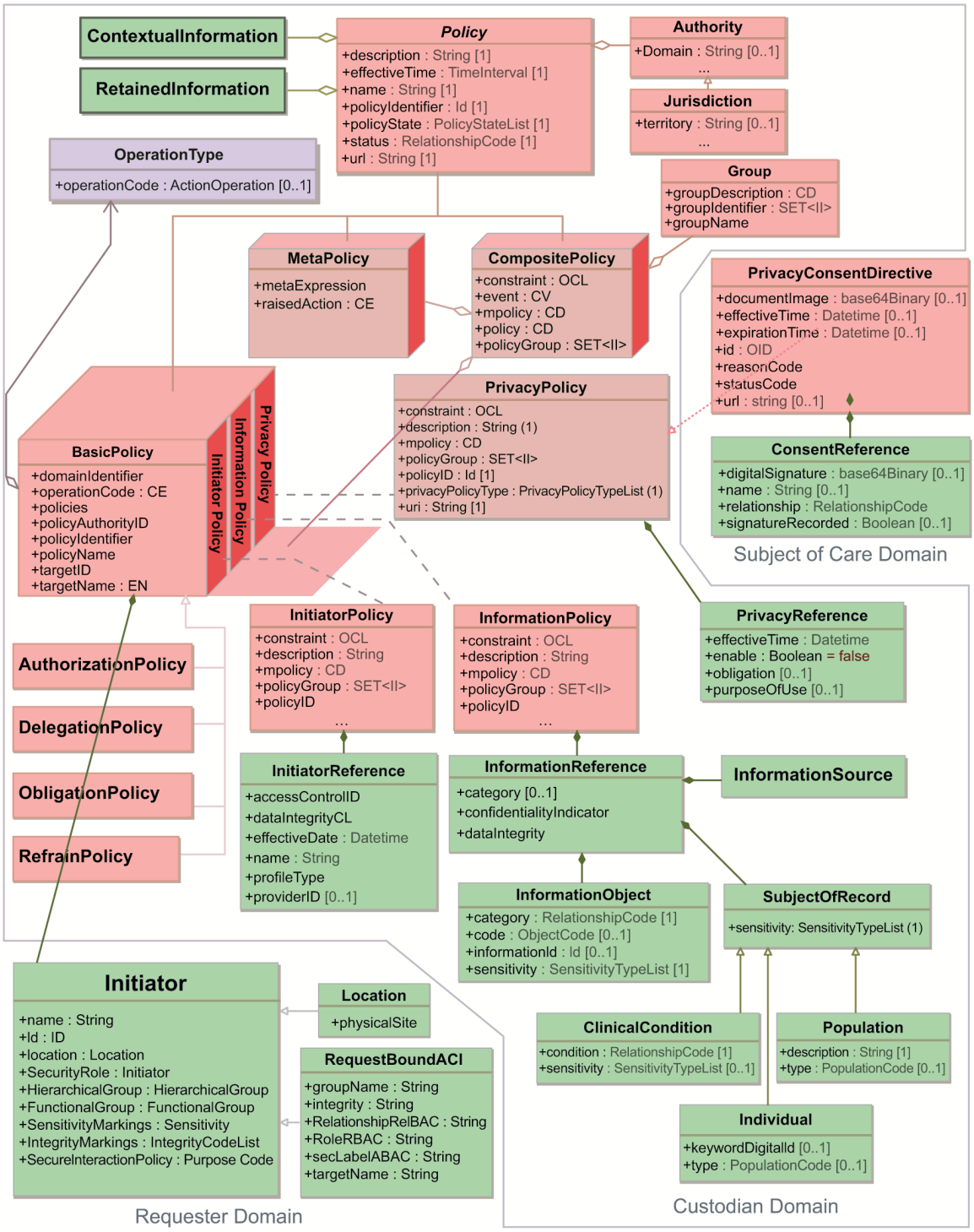
D.5 Representation and implementation of policies

As the concepts behind the architectural components are represented using the related domain ontology, policies are represented using the policy ontology standardized in ISO 22600-2:2014 Health Informatics—Privilege Management and Access Control (Figure 5) [B18]. ISO 22600 describes and explains requirements, architectures, and models as well as practical implementations for privilege management and access control in cross-domain information systems including an ontology for formally representing policies. Having been the first ISO specification deploying the interoperability reference architecture in the early 2000s, it can also be utilized for managing privacy and security, e.g., in the context of GDPR [B9]. The accurate architecturally and conceptually represented policies may be harmonized by ontology mapping. The resulting use case-specific policy at run time may be transformed in an architecturally correct and consistent way into the corresponding viewpoints of ISO 10746 Information technology—Open distributed processing—Reference model, thereby re-using and adapting existing specifications (e.g., the machine-readable personal privacy terms specified). Policy implementation examples have been defined in ISO 22600-3:2014 [B19].

The described process may be automated. The same holds for transforming the cross-domain, harmonized, consistent informational representation of the complex business system into the different ISO/IEC 10746 views for analyzing, designing, implementing, and maintaining the related ICT solution.

The presented approach has been successfully deployed in several cross-domain ISO specifications, such as ISO 22600 Health Informatics—Privilege Management and Access Control, ISO 21298 Health

Informatics—Functional and Structural Roles, and HL7 Composite Security and Privacy Domain Analysis Model. The most comprehensive deployment of ISO 23903 and ISO 22600 has been standardized in the HL7 Privacy and Security Logical Data Model, Release 1, June 2021. This standard advances and replaces the aforementioned HL7 Composite Security and Privacy Domain Analysis Model by implementable specifications. Figure D.5 presents the Privacy and Security Logical Data Model classes for policies in specific contexts. For defining trust in a policy controlling the behavior of an ecosystem, different trust models may be applied (more information on trust models see Ruotsalainen and Blobel, “Transformed health ecosystems—Challenges for security, privacy, and trust [B32]).



Reprinted with permission from Health Level Seven® International,
HL7 Privacy and Security Logical Data Model, Release 1, June 2021

Figure D.5—Logical data model of classes for representing policies in specific contexts

The feasibility of the interoperability and integration reference architecture has been practically demonstrated for automatically harmonizing HL7 version 2.x and HL7 version 3 specifications or for automatically designing inter-domain Web services to facilitate multi-disciplinary approaches to Type 2 Diabetes Care management. The approach also allows a comparative analysis and evaluation as well as harmonization of ICT Enterprise Architectures. A deep introduction and summary of the presented approach for health and social care ecosystems is provided in HL7 version 2.x and HL7 version 3.

Annex E

(informative)

Bibliography

Bibliographical references are resources that provide additional or helpful material but do not need to be understood or used to implement this standard. Reference to these resources is made for informational use only.

The following reference documents are, depending on the context and extent of development, helpful for the application of this document (i.e., they must be understood and used, so each referenced document is cited in the text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

[B1] Blobel, B., F. Oemig, P. Ruotsalainen, M. Brochhausen, K.W. Sexton, and M. Giacomini, "The representational challenge of integration and interoperability in transformed health ecosystems," Journal of Personalized Medicine, vol. 15, no. 1, 4 (21 pgs.), 2025. https://doi.org/10.3390/jpm15010004.

[B2] Blobel, B., P. Ruotsalainen, M. Brochhausen, E. Prestes, and M.A. Houghtaling, "Designing and managing advanced, intelligent and ethical health and social care ecosystems," Journal of Personalized Medicine, vol. 13, no. 8, 1209, 2023 (18 pgs.). https://doi.org/10.3390/jpm13081209.

[B3] California Consumer Privacy Act. https://oag.ca.gov/privacy/ccpa.

[B4] Cockburn, A., Writing Effective Use Cases. Boston: Addison-Wesley, 2001.

[B5] Data Privacy Vocabulary (DPV), Version 1, Dec. 2022. https://w3c.github.io/dpv/1.0/dpv/.

[B6] The Digital Markets Act. https://digital-markets-act.ec.europa.eu/index_en

[B7] Doty, N. and T. Roessler, "'Do Not Track' standards for the Web: The work is starting." https://www.w3.org/blog/2011/do-not-track-standards-for-the/.

[B8] EN/ISO 13940:2016, Health informatics—System of concepts to support continuity of care.[22,23]

[B9] General Data Protection Regulation (GDPR). https://gdpr-info.eu/.

[B10] Global Compact for Migration Portal. https://www.migrationdataportal.org/global-compact-for-migration.

[B11] Global Privacy Control (GPC). https://w3c.github.io/gpc/.

[B12] HL7 Privacy and Security Logical Data Model, Release 1, June 2021.

[B13] HL7 Version 3 Domain Analysis Model: Composite Security and Privacy, Release 1, May 2020.

[B14] ICAO Doc 9303, Machine Readable Travel Documents, 8th ed. , 2021. https://www.icao.int/sites/default/files/publications/DocSeries/9303_p3_cons_en.pdf.

[B15] IEEE Std 610™-1990, IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries.[24,25]

[B16] ISO 21298:2017, Health informatics—Functional and structural roles.

[22] EN publications are available from the European Committee for Standardization (CEN) (https://www.cen.eu/).
[23] ISO publications are available from the International Organization for Standardization (https://www.iso.org/) and the American National Standards Institute (https://www.ansi.org/).
[24] IEEE standards and products are trademarks owned by The Institute of Electrical and Electronics Engineers, Incorporated.
[25] IEEE publications are available from The Institute of Electrical and Electronics Engineers (https://standards.ieee.org/).

[B17] ISO 22600-1:2014, Health informatics—Privilege management and access control—Part 1: Overview and policy management.

[B18] ISO 22600-2:2014, Health informatics—Privilege management and access control—Part 2: Formal models.

[B19] ISO 22600-3:2014, Health informatics—Privilege management and access control—Part 3: Implementations.

[B20] ISO 23903:2021, Health informatics—Interoperability and integration reference architecture—Model and framework.

[B21] ISO/HL7 21731:2014, Health informatics—HL7 version 3—Reference information model—Release 4.

[B22] ISO/IEC 10746-1:1998, Information technology—Open Distributed Processing—Reference model: Overview.

[B23] ISO/IEC 10746-2:2009, Information technology—Open Distributed Processing—Reference model: Foundations.

[B24] ISO/IEC 10746-3:2009, Information technology—Open distributed processing—Reference model: Architecture.

[B25] ISO/IEC 10746-4:1998, Information technology—Open Distributed Processing—Reference model: Architectural semantics.

[B26] Kamareddine, F., T. Laan, and R. Nederpelt, A Modern Perspective on Type Theory. New York, Kluwer Academic Publishers, 2004.

[B27] Kantara Initiative/Customer Commons User Submitted Terms Working Group: No Stalking. Exemplary Human- and Legal-readable layers. Archived at https://kantara.atlassian.net/wiki/spaces/archive/pages/3506280/User+Submitted+Term+--+UX+and+Interface+V.2+No+Stalking+Term (last updated Jul. 11 2016) and https://kantara.atlassian.net/wiki/spaces/archive/pages/3508760/User+Submitted+Terms+--+UX+and+Interface+V.1 (last updated Apr. 18 2016).

[B28] Kessler, F., "The contracts of adhesion—some thoughts about freedom of contract role of compulsion in economic transactions," Columbia Law Review, vol. 43, no. 5, pp. 629-642, Jul. 1943. https://doi.org/10.2307/1117230.

[B29] Larman, C., Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and Iterative Development, 3rd ed. Upper Saddle River, NJ: Prentice Hall PTR, 2004.

[B30] OMG Ontology Definition Metamodel V1.1. https://www.omg.org/spec/ODM/1.1/.

[B31] Pires, I.M., H.V. Denysyuk, M.V. Villasana, J. Sá, P. Lameski, I. Chorbev, E. Zdravevski, V. Trajkovik, J.F. Morgado, and N.M. Garcia, "Mobile 5P-medicine approach for cardiovascular patients," Sensors, vol. 21, no. 21, 6986 (16 pgs.), 2021. https://doi.org/10.3390/s21216986.

[B32] Ruotsalainen, P., and B. Blobel, "Future phealth ecosystem-holitic view on privacy and trust," Journal of Personalized Medicine, vol. 13, no. 7, 1048 (18 pgs.), 2023. https://doi.org/10.3390/jpm13071048.

[B33] Ruotsalainen, P., and B. Blobel, "Transformed health ecosystems—Challenges for security, privacy, and trust," Frontiers in Medicine, vol. 9, 827253 (10 pgs.), March 2022. https://doi.org/10.3389/fmed.2022.827253.

[B34] Ruotsalainen, P., B. Blobel, and S. Pohjolainen, "Privacy and trust in ehealth: A fuzzy linguistic solution for calculating the merit of service," Joural of Personalized Medicine, vol. 12, no. 5, 657 (21 pgs.), 2022. https://doi.org/10.3390/jpm12050657.

[B35] Sloan, R.H., and R. Warner, "Beyond notice and choice: Privacy, norms, and consent," Journal of High Technology Law, vol. XIV, no. 2, pp. 370-412, 2014.

[B36] User Submitted Term—UX and Interface V.2: "No Stalking" Term. https://kantara.atlassian.net/wiki/spaces/archive/pages/3506280/User+Submitted+Term+--+UX+and+Interface+V.2+No+Stalking+Term

[B37] W3C Working Group Note 17 January 2019, Tracking Preference Expression (DNT). https://www.w3.org/2011/tracking-protection/drafts/tracking-dnt.html.

[B38] Whysel, N. Usability Reference Guidelines and Metrics Paper—produced as general usability overview of the field, (UXC Working Group, edited with guidance by M. Hodder, User Experience Working Group Chair, in 2018 for Identity Ecosystem Steering Group, but now located at Kantara Initiative). https://idefregistry.edufoundation.kantarainitiative.org/idef-knowledge-base/identity-ecosystem-framework-idef/ux-guidelines-and-metrics.

[B39] Zuboff., S., The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019.

IEEE SA
STANDARDS ASSOCIATION

RAISING THE WORLD'S STANDARDS

Connect with us on:

Facebook: facebook.com/ieeesa
LinkedIn: linkedin.com/groups/1791118
Beyond Standards blog: beyondstandards.ieee.org
YouTube: youtube.com/ieeesa

standards.ieee.org
Phone: +1 732 981 0060

IEEE