

IEEE Standard for Trusted Data Matrix System Architecture

IEEE Computer Society

Developed by the
Standards Activities Board

IEEE Std 3158™-2024

STANDARDS

IEEE Standard for Trusted Data Matrix System Architecture

Developed by the

Standards Activities Board
of the
IEEE Computer Society

Approved 6 June 2024

IEEE SA Standards Board

Abstract: The system architecture for a trusted data matrix, which includes business, functional, process, and technology requirements, are specified in this standard. Based on consensus-made requirements, agreements and management tools, the trusted data matrix is a data and resource sharing digital infrastructure to facilitate trusted, secure, transparent, and accountable data sharing, exchanging, circulation, and trading among different stakeholders.

Keywords: business view, centralized mode, federated mode, functional view, IEEE 3158™, process view, system architecture, technology view, trusted data matrix

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

Copyright © 2024 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 13 December 2024. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 979-8-8557-1031-1 STD27169
Print: ISBN 979-8-8557-1032-8 STDPD27169

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <https://www.ieee.org/about/corporate/governance/p9-26.html>.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

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 and 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

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

¹Available at: <https://development.standards.ieee.org/myproject-web/public/view.html#landing>.

²Available at: <https://standards.ieee.org/about/contact/>.

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

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, neither IEEE nor its licensors waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; <https://www.copyright.com/>. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

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

³Available at: <https://ieeexplore.ieee.org/browse/standards/collection/ieee>.

⁴Available at: <https://standards.ieee.org/standard/index.html>.

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.

⁵Available at: <https://standards.ieee.org/about/sasb/patcom/materials.html>.

Participants

At the time this standard was completed, the Trusted Data Matrix Working Group had the following membership:

Sha Wei, *Chair*
Changwei Weng, *Vice Chair*
Chuan Ma, *Secretary*

Wenting Chang	Chen Jin	Yaodong Tao
Du Chen	Jun Li	Yunhe Wang
Fei Chen	Rong Li	Qiang Wei
Mingyou Chen	Xiaocui Li	Haiqin Xie
Jiabao Dong	Yidong Li	Yunlong Xie
Li'an Fan	Guanzhou Lin	Yida Xu
Fan Gao	Zheng Lin	Xiaolong Yan
Weiran Guan	Tiancheng Liu	Shuai Yang
Yunchuan Guo	Xiaoqi Ma	Min Zhang
Zhangyi Hu	Zhenjun Ma	Ziwen Zhou
Jianxin Huang	Lei Ren	Aixue Zhong
Jun Jiang	Bo Tang	Wenchao Zou

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

Fan An	Piotr Karocki	Yunhe Wang
Boon Chong Ang	Jun Li	Qiang Wei
Pin Chang	Rong Li	Sha Wei
Wenting Chang	Daozhuang Lin	Changwei Weng
Fei Chen	Guanzhou Lin	Haiqin Xie
Guorun Chen	Tiancheng Liu	Yunlong Xie
Mingyou Chen	Wei Liu	Yida Xu
Zhiman Chen	Xiaohui Liu	Xiaolong Yan
Yuqian Ding	Xin Lu	Tao Yaodong
Jiabao Dong	Chuan Ma	Yu Yuan
Chen Du	Xiaoqi Ma	Janusz Zalewski
Madhukar Gaganam	Bansi Patel	Hanning Zhang
Fan Gao	R. K. Rannow	Min Zhang
Weiran Guan	Lei Ren	Shuo Zhang
Yunchuan Guo	Jhony Sembiring	Zhen Zhang
Werner Hoelzl	Yang Shuai	Zhihai Zhao
Zhangyi Hu	Walter Struppler	Ma Zhenjun
Jianxin Huang	Qi Sun	Aixue Zhong
Jun Jiang	Bo Tang	Ziwen Zhou
Mao Junjie	Yong Wang	Wenchao Zou
	Yu Wang	

When the IEEE SA Standards Board approved this standard on 6 June 2024, it had the following membership:

David J. Law, *Chair*
Jon Walter Rosdahl, *Vice Chair*
Gary Hoffman, *Past Chair*
Alpesh Shah, *Secretary*

Sara Biyabani
Ted Burse
Stephen Dukes
Doug Edwards
J. Travis Griffith
Guido R. Hiertz
Ronald W. Hotchkiss

Hao Hu
Yousef Kimiagar
Joseph L. Koepfinger*
Howard Li
Xiaohui Liu
John Haiying Lu
Kevin W. Lu
Hiroshi Mano

Paul Nikolich
Robby Robson
Lei Wang
F. Keith Waters
Sha Wei
Philip B. Winston
Don Wright

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 3158-2024, IEEE Standard for Trusted Data Matrix System Architecture.

The trusted data matrix (TDM) is a decentralized data infrastructure that builds upon existing information networks and facilitates the entire data sharing lifecycle. The system architecture of the Trusted Data Matrix consists of four perspectives: business view, functional view, technology view and process view. The relationship between the four perspectives can be summarized as follows:

- a) The business view describes the services or business provided by different stakeholders, dividing the business into multiple activities.
- b) The functional view realizes various activities in the business view through different combinations of functions.
- c) The technology view realizes the functions in the functional view through different combinations of technological means.
- d) The process view connects different activities in the business view, fully realizing the entire business and service process.

Contents

1. Overview	11
1.1 Scope	11
1.2 Word usage	11
2. Normative references	11
3. Definitions, acronyms, and abbreviations	12
3.1 Definitions	12
3.2 Acronyms and abbreviations	14
4. System architecture	14
5. Business view	17
5.1 General	17
5.2 Centralized mode	17
5.3 Federated mode	24
6. Functional view	30
6.1 General	30
6.2 Description of modules and functions	30
6.3 Centralized mode	34
6.4 Federated mode	38
7. Technology view	43
7.1 General	43
7.2 Description of technologies	43
7.3 Relationship between technology and corresponding function	45
8. Process view	46
8.1 General	46
8.2 Centralized mode	46
8.3 Federated mode	52
Annex A (informative) Implementation view	54
Annex B (informative) Other related technology	55
Annex C (informative) XML from a process view	58
Annex D (informative) Use cases	152

IEEE Standard for Trusted Data Matrix System Architecture

1. Overview

1.1 Scope

The standard specifies the system architecture for a trusted data matrix that includes business, functional, process, and technology requirements. Based on consensus-made requirements, agreements and management tools, the trusted data matrix is a data and resource sharing digital infrastructure to facilitate trusted, secure, transparent, and accountable data sharing, exchanging, circulation and trading among different stakeholders.

1.2 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*).^{6,7}

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

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in 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.

⁶The use of the word *must* is deprecated and cannot be used when stating mandatory requirements; *must* is used only to describe unavoidable situations.

⁷The use of *will* is deprecated and cannot be used when stating mandatory requirements; *will* is only used in statements of fact.

ISO/IEC/IEEE 42010:2022, Software, systems, and enterprise—Architecture description.^{8,9,10}

3. Definitions, acronyms, and abbreviations

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.¹¹

compliance service provider: A third party service provider that offers security, compliance, and fairness-assurance services for all participants in the trusted data matrix, including identity management service providers, authentication service providers, transaction audit service providers, logging service providers, regulatory entities, and trustworthiness management service providers.

data asset: Refers to any valuable and strategically significant data or data-related resource for an organization or individual.

NOTE—Data assets can include raw data, processed information, databases, data models, data sets, data visualizations, and other data-related artifacts that contribute to the organization’s decision-making, operations, and overall business value.¹²

data collection: The systematic process of gathering and capturing information from diverse sources to create a data set or gain knowledge about specific phenomena.

NOTE 1—Data collection involves selecting and defining data variables, designing data collection instruments (e.g., surveys, questionnaires, sensors), and implementing methods to retrieve or record the data.

NOTE 2—Data collection is a fundamental step in data management and analysis, and the quality of the collected data directly influences the validity and reliability of subsequent data-driven activities.

data consumer: A party or entity that accesses, retrieves, or utilizes data from a system or ecosystem for analysis, processing, or decision-making purposes.

data deletion: The activity of permanently and securely erasing data from storage media or systems to render it unrecoverable and prevent unauthorized access.

NOTE—Data deletion helps to ensure that sensitive or confidential information is completely removed from the devices or storage devices of the data consumer before they are discarded, repurposed, or transferred to other parties. The data stored at the data provider and the third-party service provider is preserved.

data exchange: The process of transferring or sharing data between different systems, applications, or entities in a standardized and interoperable manner.

NOTE—Data exchange enables seamless communication and collaboration by allowing data to flow across diverse platforms and environments.

⁸ISO/IEC publications are available from the International Organization for Standardization (<https://www.iso.org/>), the International Electrotechnical Commission (<https://www.iec.ch>), and the American National Standards Institute (<https://www.ansi.org/>).

⁹IEEE publications are available from the Institute of Electrical and Electronics Engineers, Inc., (<https://standards.ieee.org/>).

¹⁰The IEEE standards or products referred to in this clause are trademarks of The Institute of Electrical and Electronics Engineers, Inc.

¹¹*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 dictionary sign-in page.

¹²Notes in text, tables, and figures are given for information only and do not contain requirements needed to implement the standard.

data preparation: The process of cleaning, transforming, and structuring raw data to ensure its quality, consistency, suitability, and security for analysis or use in various applications.

NOTE—Data preparation involves tasks such as data cleaning, data transformation, data integration, and data formatting to prepare the data for further processing, analysis, or modeling.

data pre-process: The systematic and essential step in data analysis and machine learning that involves cleaning, transforming, and preparing raw data to make it suitable for further analysis or modeling.

NOTE—The aim of data pre-processing is to address issues such as missing values, data inconsistencies, and irrelevant features before publishing, ensuring that the data is of high quality and in a format that can be effectively used by algorithms or statistical techniques.

data provider: A party or entity responsible for generating, collecting, or supplying data to a system or ecosystem.

data publishing: The process of making data sets, research findings, or other data-related resources available to a wider audience.

NOTE—Data publishing involves the dissemination of data to promote transparency, collaboration, and reproducibility in scientific research, business, or any domain that generates and utilizes data.

data transmission: The process of transferring digital information, such as text, images, or multimedia, from one device or system to another through a communication channel or network.

NOTE—Data transmission involves encoding the data, sending it over the medium, and decoding it at the receiving end to help ensure accurate and reliable data exchange.

data usage: The utilization and application of data for various purposes, such as analysis, decision-making, research, or problem-solving.

NOTE—Data usage involves extracting insights, patterns, or knowledge from the data to derive meaningful information that can drive actions and support business processes.

digital contract: A machine-readable contract that is agreed upon and formed between a data provider and a data consumer regarding the control requirements, control policies, boundary conditions, and other agreed-upon behaviors during the use of shared data.

IT infrastructure service provider: A third party service provider that offers IT infrastructure capabilities for all participants, including IT infrastructure service providers and software providers.

post-service process: The activities or operations performed on data or information after a service has been provided or completed.

NOTE—Post-service processing involves data analysis, reporting, archiving, or other post-service tasks that aim to evaluate the service's performance, gather insights, or maintain records for future reference, which can derive value or knowledge from the data generated during the service and help to ensure proper documentation and closure of the service-related activities.

supervisor: An authority or governing party or entity which is responsible for overseeing and enforcing compliance with data management practices, policies, and regulations within a system or ecosystem.

NOTE 1—The role of the supervisor/regulator involves ensuring that data handling and processing activities adhere to relevant legal requirements, industry standards, and ethical guidelines.

NOTE 2—The supervisor/regulator may have the power to monitor data operations, investigate potential violations, and impose penalties or corrective actions when necessary to maintain data integrity, security, and privacy.

third party service provider: An entity or organization providing services, resources, or tools to other parties within a system or ecosystem.

NOTE 1—Third-party service providers are generally distinct from the primary data owners and users but collaborate with them to improve data-related operations and functionalities.

NOTE 2—The services provided by third-party service providers may encompass data storage, processing, analysis, authentication, or other specialized tasks associated with data management or utilization.

transaction service provider: A third-party service provider that offers services for data transactions, including metadata query, transaction intermediary, application market, and transaction clearing.

trusted data matrix (TDM): A decentralized data infrastructure that builds upon existing information networks and facilitates the entire data sharing lifecycle.

value added service provider: A third-party service provider that offers value-added services, including data identification, resolution services, algorithm models, computing services (e.g., secure multi-party computation, federated learning, privacy computing), and data-processing apps.

3.2 Acronyms and abbreviations

BPMN	business process modeling notation
DRG	diagnosis-related group
MPC	secure multi-party computation
TEE	trusted execution environment
XML	extensible markup language

4. System architecture

This standard follows an architectural study carried out by ISO/IEC/IEEE 42010:2022.¹³ Data sharing is a process that involves the authorization of data owners to allow others to access, use, and disseminate their data. This practice can encourage collaboration, innovation, and enhance service delivery. The trusted data matrix (TDM) is a decentralized data infrastructure that builds upon existing information networks and facilitates the entire data sharing lifecycle. It helps to ensure the confirmation, fulfillment, and maintenance of digital contracts through systematic technical arrangements, addressing security and trust issues among data providers, consumers, third-party service providers, regulators, and other entities.

As illustrated in [Figure 1](#), the TDM system's architecture involves four key stakeholder types: data providers, data consumers, third-party service providers, and regulators, respectively. The types of data shared in the system include public data, enterprise data, personal data, and other data. In real-world scenarios, there are generally two patterns of data sharing, i.e., centralized and federated. In the centralized mode (CM), the following applies:

- The data provider sends metadata to a third-party service provider, which is then cataloged in a data catalog.

¹³Information on references can be found in [Clause 2](#).

- The data provider and the data consumer conduct supply and demand docking and contract negotiations on the system provided by the third-party service provider, and the third-party service provider provides digital contract evidence. Generally, the third-party service provider will also generate data usage control policies based on the digital contract and send them to the data consumer for deployment.
- After the data is used and deleted by the data consumer, the third-party service provider will provide clearing, billing, and other services.
- The records in the entire data sharing process are generally stored and certified by the third-party service provider.

In the federated mode (FM), the following applies:

- The data provider publishes its own data catalog.
- The data provider and the data consumer conduct supply and demand docking and contract negotiations by themselves. Generally, the data provider generates data usage control policies based on the digital contract and sends them to the data consumer for deployment.
- After the data is used and deleted by the data consumer, the data provider and data consumer will carry out clearing, billing and other activities by themselves.
- If necessary, the third-party service provider may be invited to provide identity authentication, digital contract and records certification, and other services.

In both modes, data is directly shared between the data provider and the data consumer. In some circumstances, when either data provider or data consumer requires additional value-added services, the data is also shared with value added service provider. Hence, the data usage policies will also be applied to value added service providers.

This standard delineates the TDM system's architecture through four perspectives: business view, functional view, process view, and technology view, as shown in [Figure 1](#). The business view describes the services or business provided by different stakeholders, dividing the business into multiple activities. The functional view realizes various activities in the business view through different combinations of functions. The technology view realizes the functions in the functional view through different combinations of technological means. The process view connects different activities in the business view, fully realizing the entire business and service process. The four architectural views are further explained in the details that follow.

The business view depicts the services and businesses offered or received by various stakeholders through the TDM system, along with the crucial activities carried out during the process of delivering or receiving these services and businesses.

The functional view illustrates the system functions necessary for the TDM system to support the services provided or received. To achieve efficient integration of functions, the standard categorizes different functions into various modules. The functional view enables different activities in the business view through various combinations of functions, detailing the specific functionality required for each activity.

The technology view introduces the primary core technologies employed in the TDM system and explains the technologies needed to realize the functions in conjunction with each functional module in the functional view.

The process view demonstrates how to effectively link different activities of the TDM system to accomplish the main processes of various services.

The functions in the functional view enable the execution of activities in the business view, while the process view connects these activities based on the distinctions of related functions in different business scenarios.

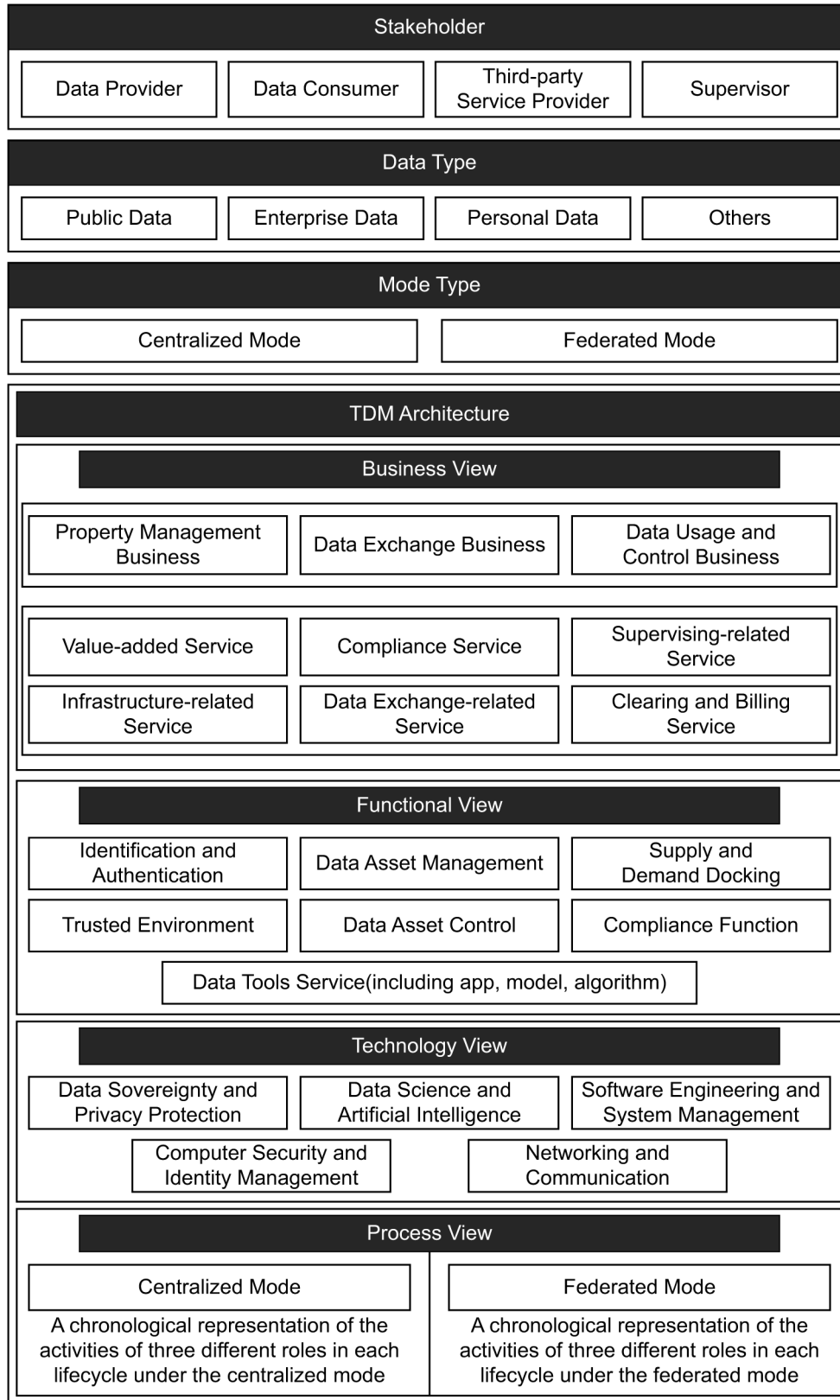


Figure 1—System architecture of trusted data matrix

5. Business view

5.1 General

The business view covers a spectrum of services and activities essential to the TDM system, including property management, data exchange, data usage and control, clearing and billing, supervisory services, value-added services, compliance, and infrastructure-related services. This perspective details the services and activities provided and utilized by different stakeholders within the TDM system. The business view of TDM is defined along the following two dimensions:

- a) Horizontal axis: Represents the data sharing process, encompassing stages like data collection, data pre-processing, data publishing, data exchange, data preparation, data transmission, data usage, data deletion, and post-service processing.
- b) Vertical axis: Denotes the stakeholders involved, which include data providers, data consumers, supervisors, and third-party service providers. Within each quadrant, the stakeholder activities are described during specific data phases.

For instance, during the data pre-processing phase, data providers handle the declaration and registration of data attributes, while supervisors oversee regulatory services. Third-party service providers offer services like logging, evaluation, computational power, data identification, and catalog management.

5.2 Centralized mode

Figure 2 illustrates the business view of the TDM in its centralized mode. In centralized mode, the distinct roles and responsibilities of the data provider, data consumer, and third-party service provider are outlined next. Table 3 describes in detail the definitions, code names, and information related to whether these activities are mandatory or optional for the above key activities of each stakeholder in the centralized mode.

Data providers engage in activities including the following, as shown in detail in Table 1:

- a) Property management business (AP1):
 - Declare and register data property (AP11)
- b) Data exchange-related business (AP2):
 - Negotiate contract (AP21)
 - Generate control policy (AP22)
 - Confirm control policy (AP23)
 - Record exchange information (AP24)
 - Evaluate the service (AP25)
- c) Data usage and control business (AP3):
 - Prepare data (AP31)
 - Send data (AP32)
 - Utilize data-tools service (AP33)
 - Coordinate data usage information (AP34)
 - Record usage information and control information (AP35)
 - Prepare clearing materials (AP36)

Data consumers, on the other hand, engage in the following:

- a) Data exchange-related business (AC1):
 - Provide data use request (AC11)
 - Negotiate contract (AC12)
 - Confirm control policy (AC13)
 - Record exchange information (AC14)
 - Evaluate the service (AC15)
- b) Data usage and control business (AC2):
 - Receive and store data (AC21)
 - Use data (AC22)
 - Utilize data-tools service (AC23)
 - Data usage control (AC24)
 - Record usage information and control information (AC25)
 - Prepare clearing materials (AC26)
 - Data deletion (AC27)

Supervisors engage in activities that include the following:

- a) Supervising-related service (AS1):
 - Regulatory service (AS11)
 - Arbitrating service (AS12)

Third-party service providers offer a spectrum of services, categorized into the following five main types:

- a) Value-added service (AT1):
 - Data-tools service (AT11)
 - Specific computing service (AT12)
 - Data usage control (AT13)
- b) Compliance service (AT2):
 - Conformity assessment service (AT21)
 - Record-related service (AT22)
 - Data deletion service (AT23)
 - Audit service (AT24)
- c) Infrastructure-related service (AT3):
 - Transmission service (AT31)
 - Computing power service (AT32)
 - Storage service (AT33)
- d) Data exchange-related service (AT4):

- Data identification service (AT41)
- Data catalog management service (AT42)
- Contract-related service (AT43)
- Evaluation service (AT44)
- e) Clearing and billing service (AT5):
 - Clearing service (AT51)
 - Billing service (AT52)

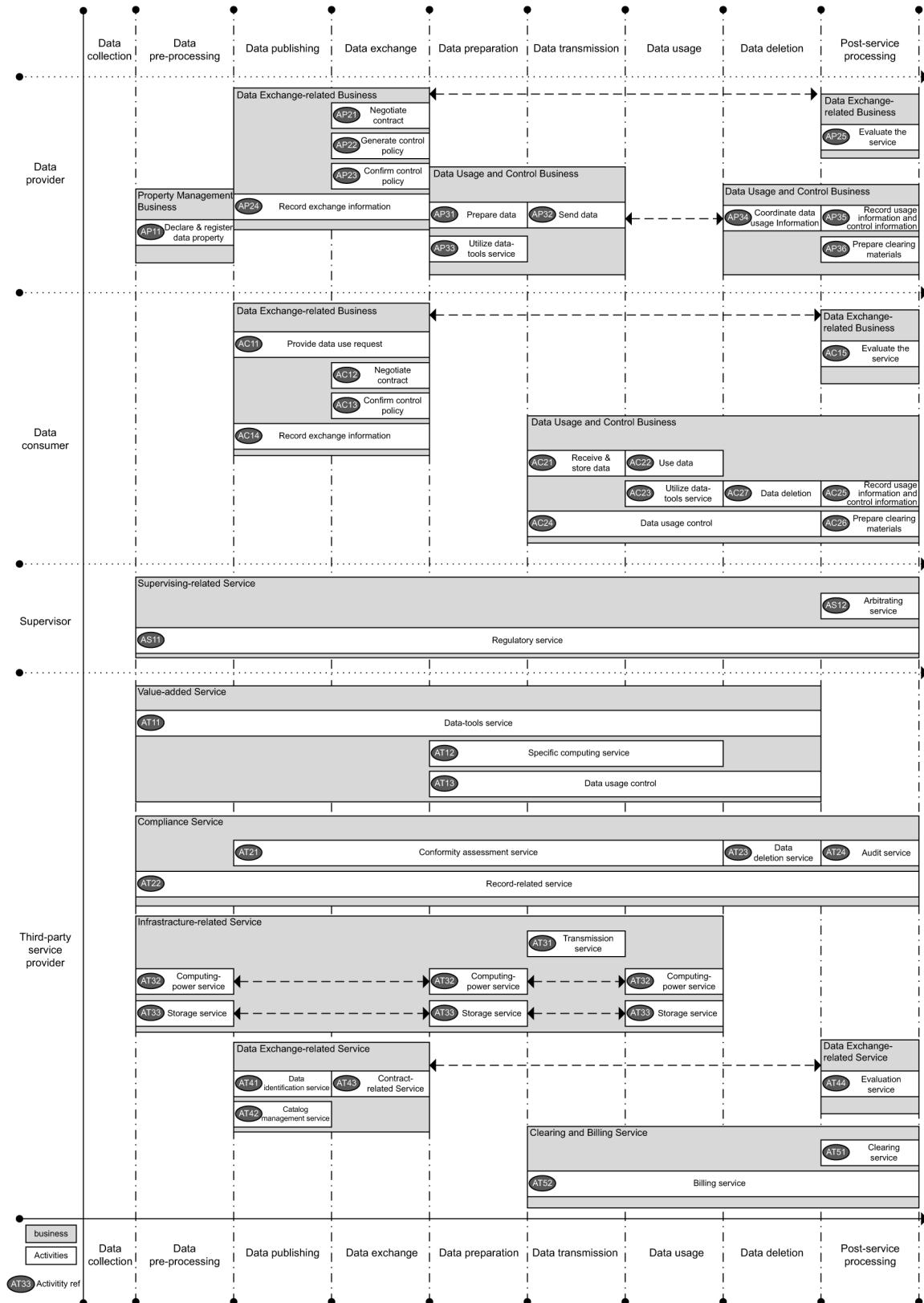


Figure 2—Business view of centralized mode

Table 1—Business description in centralized mode

Stakeholder	Business	Activity	Definition	Code name	Mandatory/Optional
Data provider	Property management business (AP1)	Declare and register data properly	The data provider shall declare and register their data property for transparency and protection.	AP11	Mandatory
	Data exchange business (AP2)	Negotiate contract	The data provider shall negotiate terms and conditions of data sharing with other stakeholders.	AP21	Mandatory
		Generate control policy	The data provider should create a policy for data usage control.	AP22	Optional
		Confirm control policy	The data provider shall agree to the control policy which comes from the contract.	AP23	Mandatory
		Record exchange information	Record of data exchange information shall be maintained for future reference and audit.	AP24	Mandatory
		Evaluate the service	The data provider should evaluate the completed service.	AP25	Optional
	Data usage and control business (AP3)	Prepare data	The data provider shall change the form of data for sharing or exchange.	AP31	Mandatory
		Send data	The data provider shall send data to the consumer.	AP32	Mandatory
		Utilize data-tools service	The data provider should use data tools for data processing and analysis.	AP33	Optional
		Coordinate data usage information	The data provider shall synchronously receive and respond to data usage information from the data consumer.	AP34	Mandatory
		Record usage information and control information	Record of data usage and control information shall be maintained.	AP35	Mandatory
		Prepare clearing materials	The data provider shall prepare the document necessary for the clearing service.	AP36	Mandatory

Table continues

Table 1—Business description in centralized mode (continued)

Stakeholder	Business	Activity	Definition	Code name	Mandatory/Optional
Data consumer	Data exchange business (AC1)	Provide data use request	The data consumer shall browse the catalog of available data and submit a data use request.	AC11	Mandatory
		Negotiate contract	The data consumer shall negotiate terms and conditions of data sharing with other stakeholders.	AC12	Mandatory
		Confirm control policy	The data consumer shall agree to the control policy which is proposed by the data provider or the contract.	AC13	Mandatory
		Record exchange information	Record of data exchange information shall be maintained for future reference and audit.	AC14	Mandatory
	Data usage and control business (AC2)	Evaluate the service	The data consumer should evaluate the completed service.	AC15	Optional
		Receive and store data	The data consumer shall receive and store the data securely.	AC21	Mandatory
		Use data	The data consumer shall use the data under data control policy.	AC22	Mandatory
		Utilize data-tools service	The data consumer should use data tools for data processing and analysis.	AC23	Optional
		Data usage control	The data consumer shall control the data usage with control policy.	AC24	Mandatory
		Record usage information and control information	The data consumer shall record the data usage information and control information.	AC25	Mandatory
		Prepare clearing materials	The data consumer shall prepare the document necessary for the clearing service.	AC26	Mandatory
		Data deletion	The data consumer shall delete the data after business is finished.	AC27	Mandatory
Supervisor	Supervising-related service (AS1)	Regulatory service	The supervisor shall offer regulatory service to ensure regulatory compliance.	AS11	Mandatory
		Arbitrating service	The supervisor should offer arbitration service in case of disputes.	AS12	Optional

Table continues

Table 1—Business description in centralized mode (continued)

Stakeholder	Business	Activity	Definition	Code name	Mandatory/Optional
Third-party service provider	Value-added service (AT1)	Data-tools service	The third-party service provider should offer tools for data processing.	AT11	Optional
		Specific computing service	The third-party service provider should offer specific computation capabilities.	AT12	Optional
		Data usage control	The third-party service provider should control the data usage with control policy when the data processing is completed.	AT13	Optional
	Compliance service (AT2)	Conformity assessment service	The third-party service provider shall conduct testing and certification to ensure standards are met, and include the data quality testing, the data-tools testing, digital identity, etc.	AT21	Mandatory
		Record-related service	The third-party service provider shall offer services related to log maintenance and analysis.	AT22	Mandatory
		Data deletion service	The third-party service provider shall offer data deletion and deletion effect evaluation services.	AT23	Mandatory
		Audit service	The third-party service provider shall perform audits to ensure compliance.	AT24	Mandatory
	Infrastructure-related service (AT3)	Transmission service	The third-party service provider should offer data transmission services.	AT31	Optional
		Computing-power service	The third-party service provider should offer computational resources.	AT32	Optional
		Storage service	The third-party service provider should offer data storage services.	AT33	Optional
	Data exchange-related service (AT4)	Data identification service	The third-party service provider shall offer services to identify and categorize data.	AT41	Mandatory
		Data catalog management service	The third-party service provider shall manage the catalog of available data.	AT42	Mandatory
		Contract-related service	The third-party service provider shall offer services related to the creation, negotiation, and maintenance of contracts.	AT43	Mandatory
	Clearing and billing service (AT5)	Evaluation service	The third-party service provider should offer services for the data provider and consumer to evaluate the quality of data sharing, data exchange, or data usage.	AT44	Optional
		Clearing service	The third-party service provider shall offer clearing service of data sharing, data exchange, or data usage.	AT51	Mandatory
		Billing service	The third-party service provider should manage billing and settle the payment.	AT52	Optional

5.3 Federated mode

Figure 3 illustrates the business view of the TDM in its federated mode. The gray shadow represents the stage of business coverage, and the white background represents the scope of activity. However, in AT1, AT2, and AT3, the activity scope covers the entire data life cycle. The scenario targeted by this model is that the entire data circulation scheme does not overly rely on the participation of third-party service providers, and only certain necessary services can be used to complete reliable data circulation.

In federated mode, third-party service providers no longer provide data exchange-related services and metering and billing services but still provide value-added services (optional), compliance services, and infrastructure-related services.

An explanatory note to Figure 3 is shown in Table 2, which describes in detail the definitions, code names, and information related to whether they are mandatory or optional for the key activities involved in the conduct of business, or the provision of services by the various stakeholders in the federal mode.

Data providers engage in activities including the following:

- a) Property management business (AP1):
 - Declare and register data property (AP11)
- b) Data exchange-related business (AP2):
 - Provide data catalog service (AP21)
 - Negotiate contract (AP22)
 - Confirm control policy (AP23)
 - Record exchange information (AP24)
 - Evaluate the service (AP25)
- c) Data usage and control business (AP3):
 - Prepare data (AP31)
 - Send data (AP32)
 - Utilize data-tools service (AP33)
 - Coordinate data usage information (AP34)
 - Record usage information and control information (AP35)
 - Prepare clearing materials (AP36)
- d) Clearing and billing service (AP4):
 - Clearing service (AP41)
 - Billing service (AP42)

Data consumers, on the other hand, engage in the following:

- a) Data exchange-related business (AC1):
 - Provide data use request (AC11)
 - Negotiate contract (AC12)
 - Confirm control policy (AC13)

- Record exchange information (AC14)
- Evaluate the service (AC15)
- b) Data usage and control business (AC2):
 - Receive and store data (AC21)
 - Use data (AC22)
 - Utilize data-tools service (AC23)
 - Data usage control (AC24)
 - Record usage information and control information (AC25)
 - Prepare clearing materials (AC26)
 - Data deletion (AC27)

Supervisors engage in activities that include the following:

- a) Supervising-related service (AS1):
 - Regulatory service (AS11)
 - Arbitrating service (AS12)

Third-party service providers offer a spectrum of services, categorized into the following five main types:

- a) Value-added service (AT1):
 - Data-tools service (AT11)
 - Specific computing service (AT12)
- b) Compliance service (AT2):
 - Conformity assessment service (AT21)
 - Record-related service (AT22)
 - Audit service (AT23)
- c) Infrastructure-related service (AT3):
 - Transmission service (AT31)
 - Computing power service (AT32)
 - Storage service (AT33)
- d) Data exchange-related service (AT4):
 - Data identification service (AT41)
 - Data catalog management service (AT42)
 - Contract-related service (AT43)

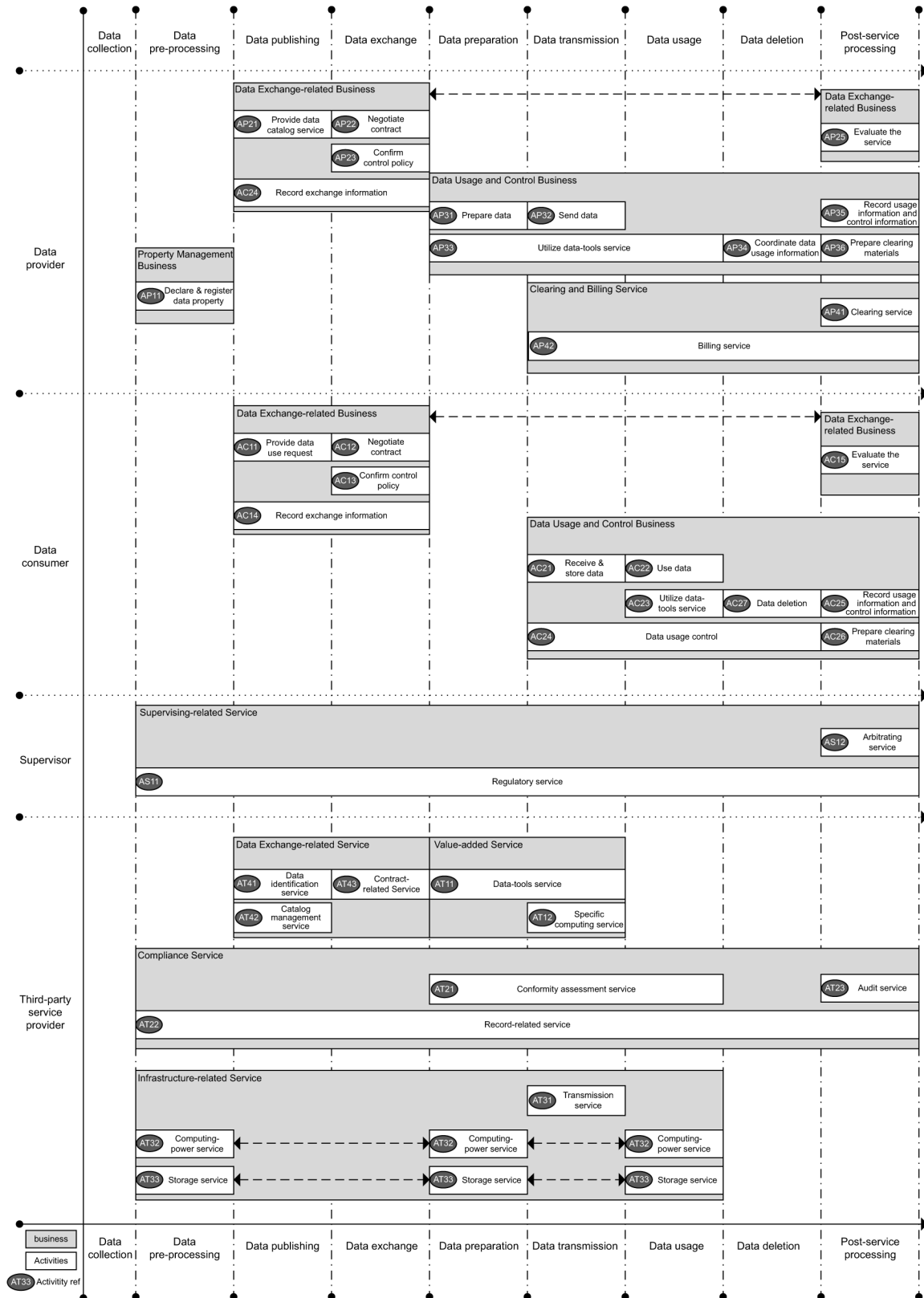


Figure 3—Business view of federated mode

Table 2—Business description in federated mode

Stakeholder	Business	Activity	Definition	Code name	Mandatory/Optional
Data provider	Property management business (AP1)	Declare and register data property	The data provider shall declare and register their data property for transparency and protection.	AP11	Mandatory
	Data exchange business (AP2)	Provide data catalog service	The data provider shall offer a catalog of their available data for exchange.	AP21	Mandatory
		Negotiate contract	The data provider shall negotiate terms and conditions of data sharing with other stakeholders.	AP22	Mandatory
		Generate control policy	The data provider shall create a policy to control the use of their data.	AP23	Mandatory
		Record exchange information	Record of data exchanges shall be maintained for future reference and audit.	AP24	Mandatory
	Data usage and control business (AP3)	Evaluate the service	The data provider should evaluate the completed service.	AP25	Optional
		Prepare data	The data provider shall change the form of data for sharing or exchange.	AP31	Mandatory
		Send data	The data provider shall send data to the consumer.	AP32	Mandatory
		Utilize data-tools service	The data provider should use data-tools for data processing and analysis.	AP33	Optional
	Clearing and billing service (AP4)	Coordinate data usage information	The data provider shall synchronously receive and respond to data usage information from the data consumer.	AP34	Mandatory
		Record usage information and control record	Record of data usage and control information shall be maintained.	AP35	Mandatory
		Prepare clearing materials	The data provider shall prepare the document necessary for the clearing service.	AP36	Mandatory
		Clearing service	The data provider shall clear the data sharing, data exchange, or data usage.	AP41	Mandatory
		Billing service	The data provider should manage billing and settle the payment.	AP42	Optional

Table continues

Table 2—Business description in federated mode (continued)

Stakeholder	Business	Activity	Definition	Code name	Mandatory/Optional
Data consumer	Data exchange business (AC1)	Provide data use request	The data consumer shall browse the catalog of available data and submit a data use request.	AC11	Mandatory
		Negotiate contract	The data consumer shall negotiate terms and conditions of data sharing with other stakeholders.	AC12	Mandatory
		Confirm control policy	The data consumer shall agree to the control policy that is proposed by the data provider or the contract.	AC13	Mandatory
		Record exchange information	Record of data exchanges shall be maintained for future reference and audit.	AC14	Mandatory
		Evaluate the service	The data consumer should evaluate the completed service.	AC15	Optional
	Data usage and control business (AC2)	Receive and store data	The data consumer shall receive and store the data securely.	AC21	Mandatory
		Use data	The data consumer shall use the data under data control policy.	AC22	Mandatory
		Utilize data-tools service	The data consumer should use data tools for data processing and analysis.	AC23	Optional
		Data usage control	The data consumer shall control the data usage with control policy.	AC24	Mandatory
		Record usage information and control information	The data consumer shall record the data usage information and control information	AC25	Mandatory
		Prepare clearing materials	The data consumer shall prepare the document necessary for the clearing service.	AC26	Mandatory
		Data deletion	The data consumer shall delete the data after business finished.	AC27	Mandatory
		Regulatory service	The supervisor shall offer regulatory service to ensure regulatory compliance.	AS11	Optional NOTE—It can be done according to two different modes and the actual situation.
		Arbitrating service	The supervisor should offer arbitration service in case of disputes.	AS12	Optional
	Supervising-related service (AS1)				

Table continues

Table 2—Business description in federated mode (continued)

Stakeholder	Business	Activity	Definition	Code name	Mandatory/Optional
Third-party service provider	Value-added service (AT1)	Data-tools service	The third-party service provider should offer tools for data processing.	AT11	Optional
		Specific computing service	The third-party service provider should offer specific computation capabilities.	AT12	Optional
	Compliance service (AT2)	Conformity assessment service	The third-party service provider shall conduct testing and certification to ensure standards are met, include the data quality testing, the data-tools testing, digital identity etc.	AT21	Mandatory NOTE—It can be done according to two different modes and the actual situation.
		Record-related service	The third-party service provider should offer services related to log maintenance and analysis.	AT22	Optional
		Audit service	The third-party service provider should perform audits to ensure compliance.	AT23	Optional
	Infrastructure-related service (AT3)	Transmission service	The third-party service provider should offer data transmission services.	AT31	Optional
		Computing-power service	The third-party service provider should offer computational resources.	AT32	Optional
		Storage service	The third-party service provider should offer data storage services.	AT33	Optional
	Data exchange-related service (AT4)	Data identification service	The third-party service provider should offer services to identify and categorize data.	AT41	Optional
		Data catalog management service	The third-party service provider should manage the catalog of available data.	AT42	Optional
		Contract-related service	The third-party service provider should offer services related to the creation, negotiation, and maintenance of contracts.	AT43	Optional

6. Functional view

6.1 General

The functional view categorizes the TDM system's required functions into distinct modules, each detailing how to support the activities outlined in the business view. The various activities from the business view are implemented through a combination of different capabilities.

6.2 Description of modules and functions

This standard segments the TDM system's functions into seven modules: Identification and authentication, data asset management, supply and demand docking, trusted environment, data asset control, data tool service, and compliance function, described as follows:

- a) The identity and authentication module encompasses functions such as user login, authentication, identity information verification, and user identity management.
- b) The data asset management module includes data asset generation, data asset identification, data asset maintenance, and other functions.
- c) The supply and demand docking module comprises data catalog management, contract management, and functions for data and service evaluation, metering, billing, and clearing.
- d) The trusted environment module includes functions such as trusted configuration, trusted execution, and trusted monitoring.
- e) The data asset control module covers data pre-processing, control strategy configuration, data status monitoring, control strategy execution, and data destruction.
- f) The data tool service module includes the installation, execution, and uninstallation functions of data tools, as well as the listing, operation, and removal functions of data tools.
- g) The compliance function module consists of logging and management, auditing, tools certification, regulatory interface, arbitration interface, and additional functions.

[Figure 4](#) illustrates the functional view of the TDM. It shows the above seven functional modules and the system functions necessary for the TDM system in each functional module to support the services provided or received at all stages of data lifecycle. The definitions, code name and other information of the specific function in each function module are described in detail in [Table 3](#).

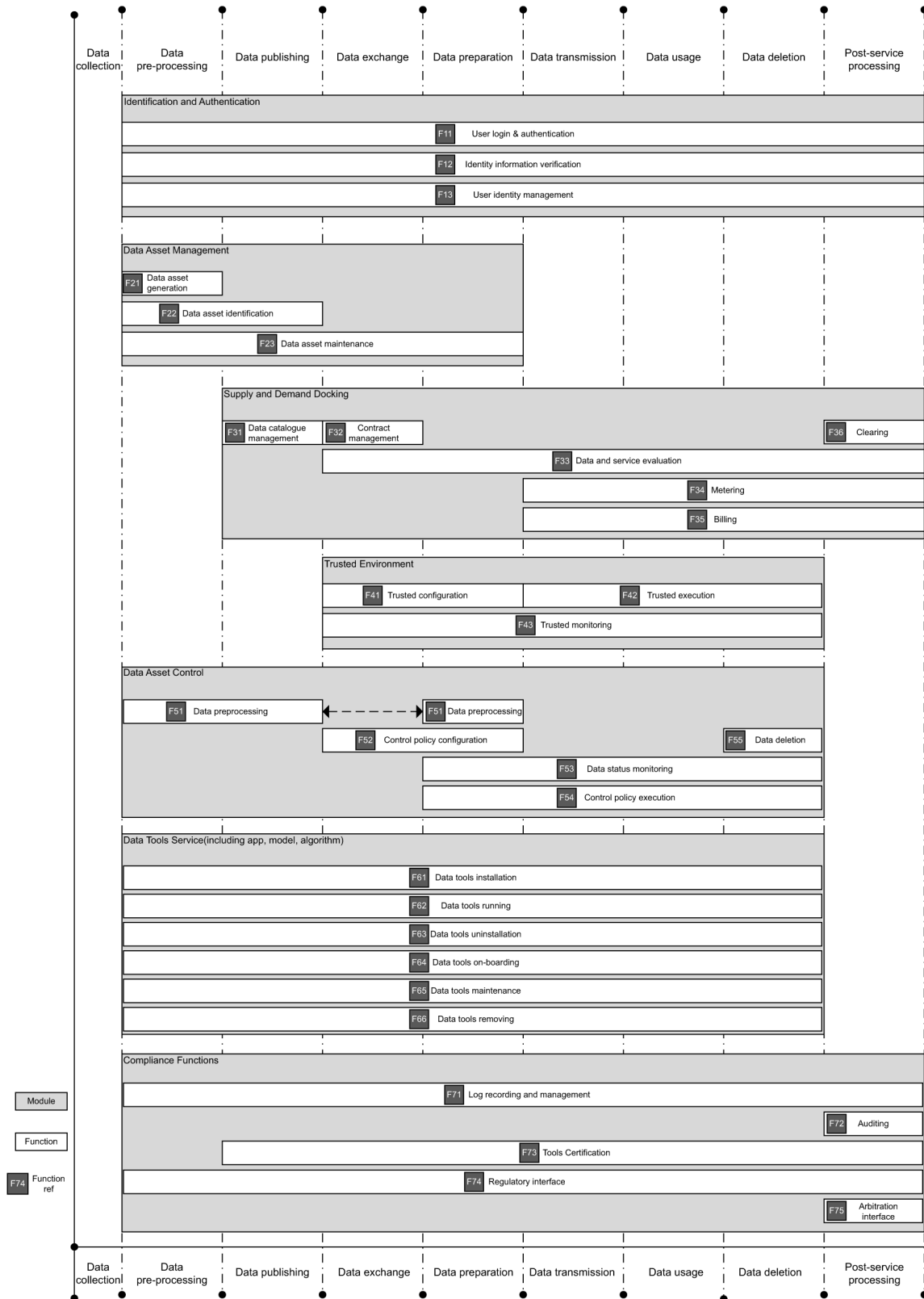


Figure 4—Function module of functional view

Table 3—Function description

Function module	Function	Definition	Code name	Mandatory/optional
Identification and authentication	User login and authentication	The users shall log in to the system and authenticate by entering a username, password, or other identity element.	F11	Mandatory
	Identity information verification	Identity verification is a method used to verify the authenticity and legitimacy of an individual's identity, typically to ensure that only authorized persons can gain access to a particular system, application, or service. It shall verify whether the provided identity information is compared with the pre-stored identity data to determine if the user is authorized to access the system.	F12	Mandatory
	User-identity management	User identity management shall manage and maintain user identity information and access rights in a system or application.	F13	Mandatory
Data asset management	Data asset generation	Data asset generation shall collect, collate, process, and transform the data from various data sources to produce valuable and usable data assets.	F21	Mandatory
	Data asset identification	Data asset identification shall identify and classify the data in an organization to determine its value, sensitivity, and importance.	F22	Mandatory
	Data asset maintenance	Data asset maintenance shall manage and protect data assets in an organization continuously to ensure data integrity, availability, reliability, and security.	F23	Mandatory
Supply and demand docking	Data catalog management	Data catalog management shall classify, organize, and manage data resources in an organization.	F31	Mandatory
	Contract management	Contract management shall manage and monitor the contracts of an organization in an effective, centralized, and standardized way.	F32	Mandatory
	Data and service evaluation	Data and service evaluation should evaluate and analyze key indicators of data and services, such as quality, security, reliability, and performance.	F33	Optional
	Metering	Metering shall calculate measurements based on data usage or consumption.	F34	Mandatory
	Billing	Billing should be calculated and charged based on data usage or consumption.	F35	Optional
	Clearing	Clearing shall verify transactions and settle accounts to ensure that all payments are accurately processed and financial obligations between parties are fulfilled.	F36	Mandatory

Table continues

Table 3—Function description (continued)

Function module	Function	Definition	Code name	Mandatory/optional
Trusted environment	Trusted configuration	Trusted configuration shall verify and protect the configuration files, software, and hardware in a computer system to ensure their integrity and trustworthiness.	F41	Mandatory
	Trusted execution	Trusted execution shall verify and protect the execution process of a computer program to ensure its trustworthiness and reliability.	F42	Mandatory
	Trusted monitoring	Trusted monitoring shall monitor and audit the operating status and activities of the computer system in real time to ensure the credibility and security of the system.	F43	Mandatory
Data asset control	Data pre-processing	Data pre-processing shall clean, transform, and integrate raw data before performing data analysis or machine learning tasks.	F51	Mandatory
	Control policy configuration	Control policy configuration function shall set and adjust control policies in a system or software.	F52	Mandatory
	Data status monitoring	Data status monitoring function shall monitor and inspect data in the system in real time or at regular intervals to ensure its accuracy, completeness, and availability.	F53	Mandatory
	Control policy execution	Control policy execution shall monitor and regulate the execution of a system or process according to pre-set rules or conditions.	F54	Mandatory
	Data deletion	The data of the data provider shall be deleted.	F55	Mandatory
Data tools service	Data tools installation	Data tools installation should ensure the normal installation of tool.	F61	Optional
	Data tools running	Data tools running should ensure the data tool runs.	F62	Optional
	Data tools uninstallation	Data tools uninstallation should ensure that the tool is uninstalled normally.	F63	Optional
	Data tools on-boarding	Data tools on-boarding should ensure that the tool is used normally online.	F64	Optional
	Data tools maintenance	Data tools maintenance should provide maintenance services such as data tool updates and upgrades.	F65	Optional
	Data tools removing	Data tools removal should ensure that the tool is completely removed.	F66	Optional

Table continues

Table 3—Function description (*continued*)

Function module	Function	Definition	Code name	Mandatory/optional
Compliance functions	Log recording and management	Log recording and management shall record the running process and results of activities to manage the system, application, or network activities.	F71	Mandatory
	Auditing	Auditing shall have the ability to monitor and record system operations, events, and activities.	F72	Mandatory
	Tools certification	Tool certification shall evaluate specific tools, software, or equipment to confirm compliance with specific standards, specifications, or requirements.	F73	Optional
	Regulatory interface	Regulatory interface should regulate software, products, or systems with reference to relevant regulations, standards, or specifications.	F74	Optional
	Arbitration interface	Arbitration interface should resolve disputes or disputes related to software, platforms, or systems.	F75	Optional

6.3 Centralized mode

In the centralized mode, data is generated, identified, maintained, and sent by data providers and contract negotiation. Control strategy formulation is completed by data providers and data consumers through relevant services provided by third-party service providers. Data processing is mainly completed by third-party service providers, and data consumers use the data. Furthermore, the entire process is governed by a data usage control policy.

Figure 5 shows the functional diagram of the business activities in the centralized mode and illustrates the specific functions required for each business activity. The functions corresponding to specific activities are described in detail in Table 4.

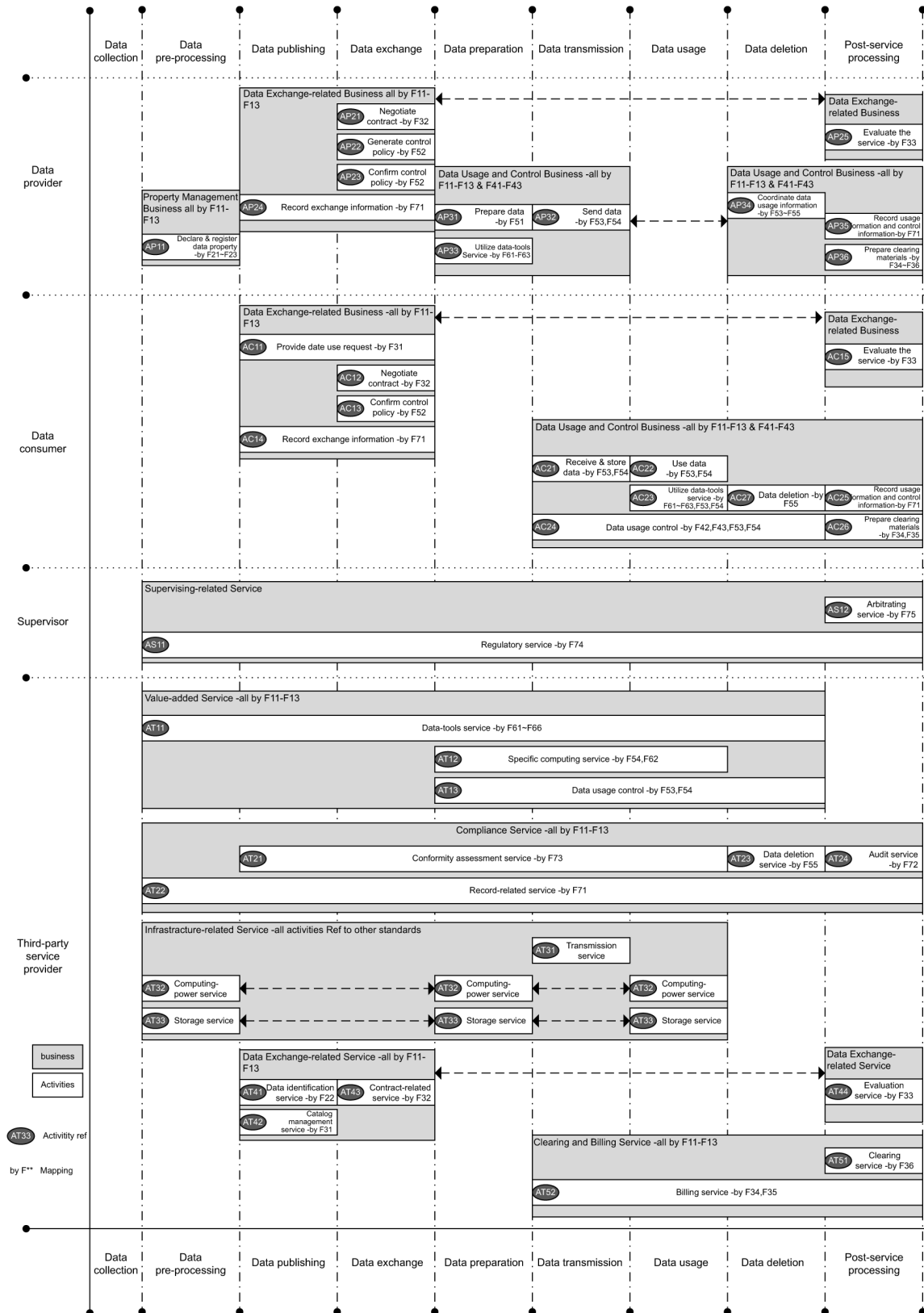


Figure 5—Functional view of centralized mode

Table 4—Business-function mapping in centralized mode

Stakeholder	Activities	Code name	Function	Code name
Data provider	Declare and register data property	AP11	Data asset generation	F21
			Data asset identification	F22
			Data asset maintenance	F23
	Negotiate contract	AP21	Contract management	F32
	Generate control policy	AP22	Control policy configuration	F52
	Confirm control policy	AP23	Control policy configuration	F52
	Record exchange information	AP24	Log recording and management	F71
	Evaluate the service	AP25	Data and service evaluation	F33
	Prepare data	AP31	Data pre-processing	F51
	Send data	AP32	Data status monitoring	F53
			Control policy execution	F54
	Utilize data-tools service	AP33	Data tools installation	F61
			Data tools running	F62
			Data tools uninstallation	F63
	Coordinate data usage information	AP34	Data status monitoring	F53
			Control policy execution	F54
			Data deletion	F55
	Record usage information and control information	AP35	Log recording and management	F71
	Prepare clearing materials	AP36	Metering	F34
			Billing	F35
			Clearing	F36

Table continues

Table 4—Business-function mapping in centralized mode (continued)

Stakeholder	Activities	Code name	Function	Code name
Data consumer	Provide data use request	AC11	Data catalog management	F31
	Negotiate contract	AC12	Contract management	F32
	Confirm control policy	AC13	Control policy configuration	F52
	Record exchange information	AC14	Log recording and management	F71
	Evaluate the service	AC15	Data and service evaluation	F33
	Receive and store data	AC21	Data status monitoring	F53
			Control policy execution	F54
	Use data	AC22	Data status monitoring	F53
			Control policy execution	F54
	Utilize data-tools service	AC23	Data tools installation	F61
			Data tools running	F62
			Data tools uninstallation	F63
			Data status monitoring	F53
			Control policy execution	F54
	Data usage control	AC24	Trusted execution	F42
			Trusted monitoring	F43
			Data status monitoring	F53
			Control policy execution	F54
	Record usage information and control information	AC25	Log recording and management	F71
	Prepare clearing materials	AC26	Metering	F34
			Billing	F35
	Data deletion	AC27	Data deletion	F55
Supervisor	Regulatory service	AS11	Regulatory interface	F74
	Arbitrating service	AS12	Arbitration interface	F75

Table continues

Table 4—Business-function mapping in centralized mode (continued)

Stakeholder	Activities	Code name	Function	Code name
Third-party service provider	Data-tools service	AT11	Data tools installation	F61
			Data tools running	F62
			Data tools uninstallation	F63
			Data tools on-boarding	F64
			Data tools maintenance	F65
			Data tools removing	F66
	Specific computing service	AT12	Control policy execution	F54
			Data tools running	F62
	Data usage control	AT13	Data status monitoring	F53
			Control policy execution	F54
	Conformity assessment service	AT21	Tools certification	F73
	Record-related service	AT22	Log recording and management	F71
	Data deletion service	AT23	Data deletion	F55
	Audit service	AT24	Auditing	F72
	Transmission service	AT31	Ref to other standards	
	Computing power service	AT32	Ref to other standards	
	Storage service	AT33	Ref to other standards	
	Data identification service	AT41	Data asset identification	F22
	Data catalog management service	AT42	Data catalog management	F31
	Contract-related service	AT43	Contract management	F32
	Evaluation service	AT44	Data and service evaluation	F33
	Clearing service	AT51	Clearing	F36
	Billing service	AT52	Metering	F34
			Billing	F35

In order to describe the implementation of business activities with different functions, this standard describes the mapping table between business activities and system functions for the previously mentioned business view.

Because some functions are common, they are not defined separately in Table 4. In detail, the functions required for the implementation of infrastructure-related services (AT31 to AT33) are beyond the scope of this standard's research. It is recommended that users refer to other standards. The functions related to identity and authentication services (F11 to F13) are used in all activities performed by data providers, data consumers, and third-party service providers, so they are marked under the service or business name. Trusted environment related services (F41 to F43) are used in data exchange related services and metering and billing services provided by third-party service providers, and all service provided by data providers and data consumers, so they are also merged and marked under the previous related services or business names.

6.4 Federated mode

In federated mode, data is generated, identified, maintained, and transmitted by the data provider. Contract negotiation and control strategy formulation are directly managed by both the data provider and the data consumer. Additionally, the data provider and data consumer may opt to utilize contract-related and data tool services offered by third-party service providers.

Figure 6 is a mapping of the TDM system functions and implemented business activities in the federated mode, similar to the centralized mode mentioned earlier. It shows the functional diagram of the business activities in the federated mode and illustrates the specific functions required for each business activity.

Table 5 describes the mapping relationship between business activities and system functions in federated mode, with reference to other standards for related common functions.

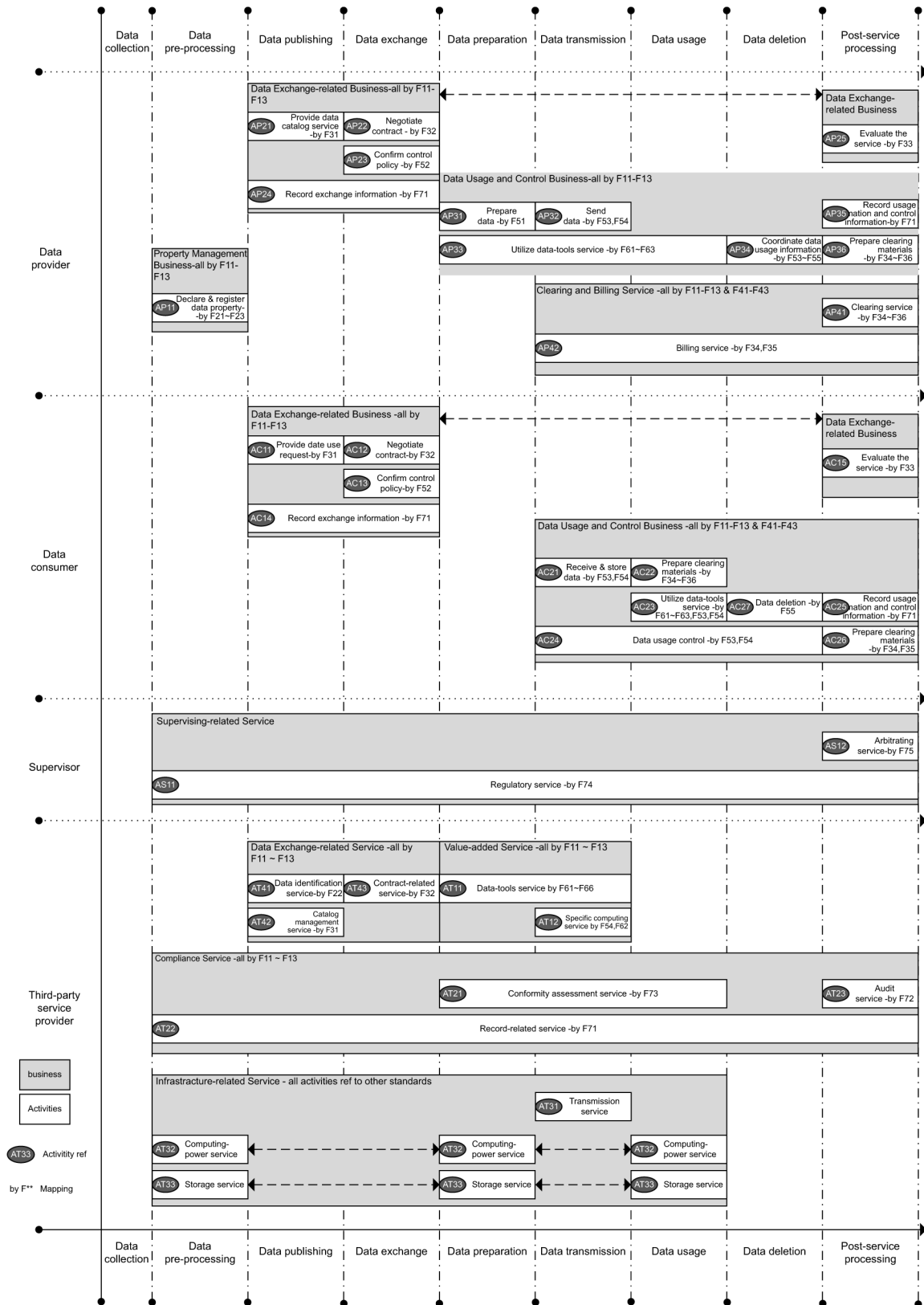


Figure 6—Functional view of federated mode

Table 5—Business function mapping in federated mode

Stakeholder	Activities	Code name	Function	Code name
Data provider	Declare and register data property	AP11	Data asset generation	F21
			Data asset identification	F22
			Data asset maintenance	F23
	Provide data catalog service	AP21	Data catalog management	F31
	Negotiate contract	AP22	Contract management	F32
	Confirm control policy	AP23	Control policy configuration	F52
	Record exchange information	AP24	Log recording and management	F71
	Evaluate the service	AP25	Data and service evaluation	F33
	Prepare data	AP31	Data pre-processing	F51
	Send data	AP32	Data status monitoring	F53
			Control policy execution	F54
	Utilize data-tools service	AP33	Data tools installation	F61
			Data tools running	F62
			Data tools uninstallation	F63
	Data usage information coordination	AP34	Data status monitoring	F53
			Control policy execution	F54
			Data deletion	F55
	Record usage information and control information	AP35	Log recording and management	F71
	Prepare clearing materials	AP36	Metering	F34
			Billing	F35
			Clearing	F36
	Clearing service	AP41	Metering	F34
			Billing	F35
			Clearing	F36
	Billing service	AP42	Metering	F34
			Billing	F35

Table continues

Table 5—Business function mapping in federated mode (continued)

Stakeholder	Activities	Code name	Function	Code name
Data consumer	Provide data use request	AC11	Data catalog management	F31
	Negotiate contract	AC12	Contract management	F32
	Confirm control policy	AC13	Control policy configuration	F52
	Record exchange information	AC14	Log recording and management	F71
	Evaluate the service	AC15	Data and service evaluation	F33
	Receive and store data	AC21	Data status monitoring	F53
			Control policy execution	F54
	Use data	AC22	Data status monitoring	F53
			Control policy execution	F54
	Utilize data-tools service	AC23	Data tools installation	F61
			Data tools running	F62
			Data tools uninstallation	F63
			Data status monitoring	F53
			Control policy execution	F54
			Data deletion	F55
	Data usage control	AC24	Data status monitoring	F53
			Control policy execution	F54
	Record usage information and control information	AC25	Log recording and management	F71
	Prepare clearing materials	AC26	Metering	F34
			Billing	F35
	Data deletion	AC27	Data deletion	F55
Supervisor	Regulatory service	AS11	Regulatory interface	F74
	Arbitrating service	AS12	Arbitration interface	F75
Third-party service provider	Data-tools service	AT11	Data tools installation	F61
			Data tools running	F62
			Data tools uninstallation	F63
			Data tools on-boarding	F64
			Data tools maintenance	F65
			Data tools removing	F66
	Specific computing service	AT12	Control policy execution	F54
			Data tools running	F62
	Conformity assessment service	AT21	Tools certification	F73
	Record-related service	AT22	Log recording and management	F71
	Audit service	AT23	Auditing	F72
	Transmission service	AT31	Ref to other standards	—
	Computing power service	AT32	Ref to other standards	—
	Storage service	AT33	Ref to other standards	—
	Data identification service	AT41	Data asset identification	F22
	Data catalog management service	AT42	Data catalog management	F31
	Contract-related service	AT43	Contract management	F32

7. Technology view

7.1 General

In the following subclause, various technologies enabling the implementation of general functionality will be explored. These technologies have been organized into five categories based on a general disciplinary system, providing a structured and comprehensive understanding of the diverse technologies involved in achieving the desired functionality. The five categories are as follows:

- Data sovereignty and privacy protection
- Data science and artificial intelligence
- Software engineering and system management
- Computer security and identity management
- Networking and communication

The core technologies related to data sovereignty and privacy protection, data science and artificial intelligence, and software engineering and system management will be explained in detail in the following text. For the detailed description of technologies related to computer security and identity management, please refer to B.4. For the detailed description of technologies related to networking and communications, please refer to B.5.

Each category encompasses a range of technologies that contribute to the overall functionality of the system. By exploring these categories and their respective technologies, a deeper understanding of the underlying mechanisms and processes driving the general functionality can be gained.

7.2 Description of technologies

7.2.1 Data sovereignty and privacy protection

Data sovereignty and privacy protection is a category of technologies and methods aimed at ensuring that data owners and users can effectively control and protect their data. These technologies and methods include access control, encryption, secure computing, etc., to help ensure the security and privacy of data during storage, transmission, and processing. The following are the core technologies in this category:

- Access control, usage control, and extended access control (T11): Access control is a method of protecting data and resources by restricting access to them, ensuring their security. Usage control is a method of restricting the use of data and resources, ensuring that they are used as intended. Extended access control builds on traditional access control, adding more features and capabilities to meet specific needs and scenarios for data sharing.
- Secure multi-party computation (T12) is a technique that allows multiple parties to complete joint computation tasks without exposing the raw data. By using MPC, parties can share and process encrypted data without worrying about data leakage.
- Federated learning (T13) is a distributed machine learning technique that enables multiple data owners to train models while protecting data privacy. Participants need not share the original data, only the model parameters and gradient information, reducing the risk of data leakage.
- Confidential computing (T14) is a technique to encrypt and protect both raw data and the computation process, ensuring that data remains encrypted during computation. It typically relies on secure hardware technologies, such as trusted execution environments (TEE) or secure processor extensions.

- Smart contract (T15) is a computer program that automatically executes contract terms, typically deployed on a blockchain. Through smart contracts, participants can achieve secure and reliable data exchange and processing without relying on third parties.
- Blockchain (T16) is a distributed database technology that ensures the security, integrity, and immutability of data through decentralization, encryption, and consensus mechanisms. Blockchain can be used for secure storage, transmission, and processing of data while protecting data privacy and sovereignty.

7.2.2 Data Science and Artificial Intelligence

Data science and artificial intelligence focuses on technologies and methods related to the analysis, processing, and understanding of data, as well as the development of intelligent systems that can learn, reason, and interact with humans. The following are the core technologies in this category:

- Data identification (T21) is the process of discovering, categorizing, and labeling data within an organization. It helps organizations understand the types of data they possess, its location, and its relevance to their operations.
- Search ranking (T22) refers to the process of ordering search results based on their relevance to a user's query. It involves algorithms and techniques that analyze various factors, such as keyword relevance, user behavior, and content quality to determine the most appropriate search results.
- Intelligent recommendation (T23) is a system that uses data analysis, machine learning, and artificial intelligence techniques to provide personalized suggestions to users. These systems analyze user preferences, behavior, and other factors to recommend relevant content, products, or services.
- Metadata repository (T24) is a centralized storage system that manages and stores metadata, which is data about data. Metadata repositories help organizations manage, discover, and understand their data assets by providing information about the structure, relationships, and usage of data.

In addition to the technologies mentioned previously, data science and artificial intelligence also include technologies such as natural language processing (T25), data wrangling (T26), anonymization (T27), randomization (T28), and data disturbance (T29). For detailed definitions and explanations, please refer to [B.2](#).

7.2.3 Software engineering and system administration

This category focuses on methods and technologies related to software development, maintenance, and management. The following are the core technologies in this category:

- Trusted execution environment (T31) is a security technology that creates an independent, protected runtime environment within a device to help ensure the secure execution of sensitive data and applications.
- Container (T32) is a lightweight virtualization technology that packages applications and their dependencies in an independent runtime environment, enabling rapid deployment, scaling, and portability of applications.

In addition to the technologies mentioned previously, software engineering and system administration also includes technologies such as virtualization (T33) and package management (T34). For detailed explanations, please refer to [B.3](#).

7.3 Relationship between technology and corresponding function

Table 6 shows the mapping relationship between functions and technologies, that is, the corresponding technologies required to achieve a specific function.

Table 6—Function-technology mapping

Functions	Technologies and code name	Description of how technologies serve corresponding functions
Identity authentication	Multi-factor authentication (T41)	Enhances security by using multiple verification methods, such as passwords, biometrics, and hardware tokens.
	Digital certificate authentication technology (T42)	Verifies user identity using digital certificates, ensuring that only legitimate users can access protected resources.
	Digital signature authentication technology (T43)	Verifies data integrity and origin using digital signatures, preventing tampering and forgery.
	OAuth (T44)	Allows third-party applications to access specific resources without sharing user credentials.
	Identity and access management (T45)	Manages user identities and permissions, ensuring that only authorized users can access protected resources.
	Distributed ID (T46)	Manages and verifies user identities using a decentralized approach, improving security and privacy protection.
	Self-sovereign identity (T47)	Empowers users to own and control their identity information, enhancing privacy protection and security.
Data asset management	Data identification (T21)	Identifies and classifies data for better management and protection.
	Metadata repository (T24)	Stores and manages metadata of data, facilitating data asset retrieval and analysis.
	Data wrangling (T26)	Cleans, transforms, and integrates data to improve data quality and usability.
	Anonymization (T27)	Removes personal identity information from data to protect user privacy.
	Randomization (T28)	Processes data randomly to reduce the risk of data leakage.
	Data disturbance (T29)	Disturbs data to protect data privacy.
Supply-demand docking	Metadata repository (T24)	Stores and manages metadata of data, facilitating data asset retrieval and analysis.
	Search ranking (T22)	Ranks search results based on relevance and other factors.
	Intelligent recommendation (T23)	Provides personalized recommendations based on user preferences and behavior.
Trusted environment	Trusted execution environment (T31)	Provides a secure environment for executing sensitive code and processing sensitive data.
	Virtualization (T33)	Creates virtual instances of hardware and software resources, improving security and resource utilization.
	Container (T32)	Packages applications and their dependencies into a single unit, improving security and portability.
	Secured gateway (T49)	Protects network traffic by filtering and monitoring data between different networks.
	Transmission source encryption (T51)	Encrypts data at the source before transmission, protecting data from eavesdropping and tampering.
	Channel encryption (T52)	Encrypts data during transmission, protecting data from eavesdropping and tampering.
	Virtual private network (T53)	Creates a secure, encrypted connection between networks, protecting data from eavesdropping and tampering.

Table continues

Table 6—Function-technology mapping (*continued*)

Functions	Technologies and code name	Description of how technologies serve corresponding functions
Data asset control	Access control, usage control, and extended access control (T11)	Manages and enforces access and usage policies for data assets.
	Smart contract (T15)	Automates the execution of predefined rules and agreements, ensuring trust and transparency.
Data service	Natural language processing (T25)	Processes and analyzes human language data, enabling better understanding and interaction with users.
	Secure multi-party computation (T12)	Enables secure computation on encrypted data from multiple parties, protecting data privacy.
	Federated learning (T13)	Trains machine learning models on decentralized data, protecting data privacy and reducing data movement.
	Confidential computing (T14)	Processes sensitive data in a secure environment, protecting data privacy and integrity.
Compliance functional modules	Security information and event management (T48)	Collects, analyzes, and correlates security events and logs, enabling better security monitoring and incident response.
	Secured gateway (T49)	Protects network traffic by filtering and monitoring data between different networks.
	Package management(T34)	Manages software packages and their dependencies, ensuring system stability and security.
	Blockchain (T16)	Provides a decentralized, tamper-proof ledger for recording transactions and data, ensuring trust and transparency.

8. Process view

8.1 General

The process view is a method of describing the interaction of role activities in the trusted data matrix, which demonstrates the dynamic characteristics of reference architecture models. The process view describes the main participants in the entire ecosystem and their collaborative relationships, as well as the flow and transformation process of data, from a global process perspective. The process view can help understand and analyze the operational mechanisms and optimization solutions of the trusted data matrix.

This clause divides the transaction process into centralized mode and federated mode based on the participation level of intermediate service providers in the entire transaction process, combined with different real-life data transaction scenarios. Centralized mode refers to the involvement of both parties in trading activities that rely on the services of intermediary service providers. Federated mode, on the other hand, refers to data trading activities where both parties do not rely heavily on the services of intermediary service providers. The details of the two modes are described in the following subclauses.

8.2 Centralized mode

Besides the supervisor, the other three stakeholders carried out dozens of activities of the centralized mode. Because there is no individual activity of data collection in the business view, the overall working flow diagram includes eight stages, shown in [Figure 7](#), [Figure 8](#), and [Figure 9](#). The illustrations of images are based on the business process modeling notation (BPMN) 2.0 model.

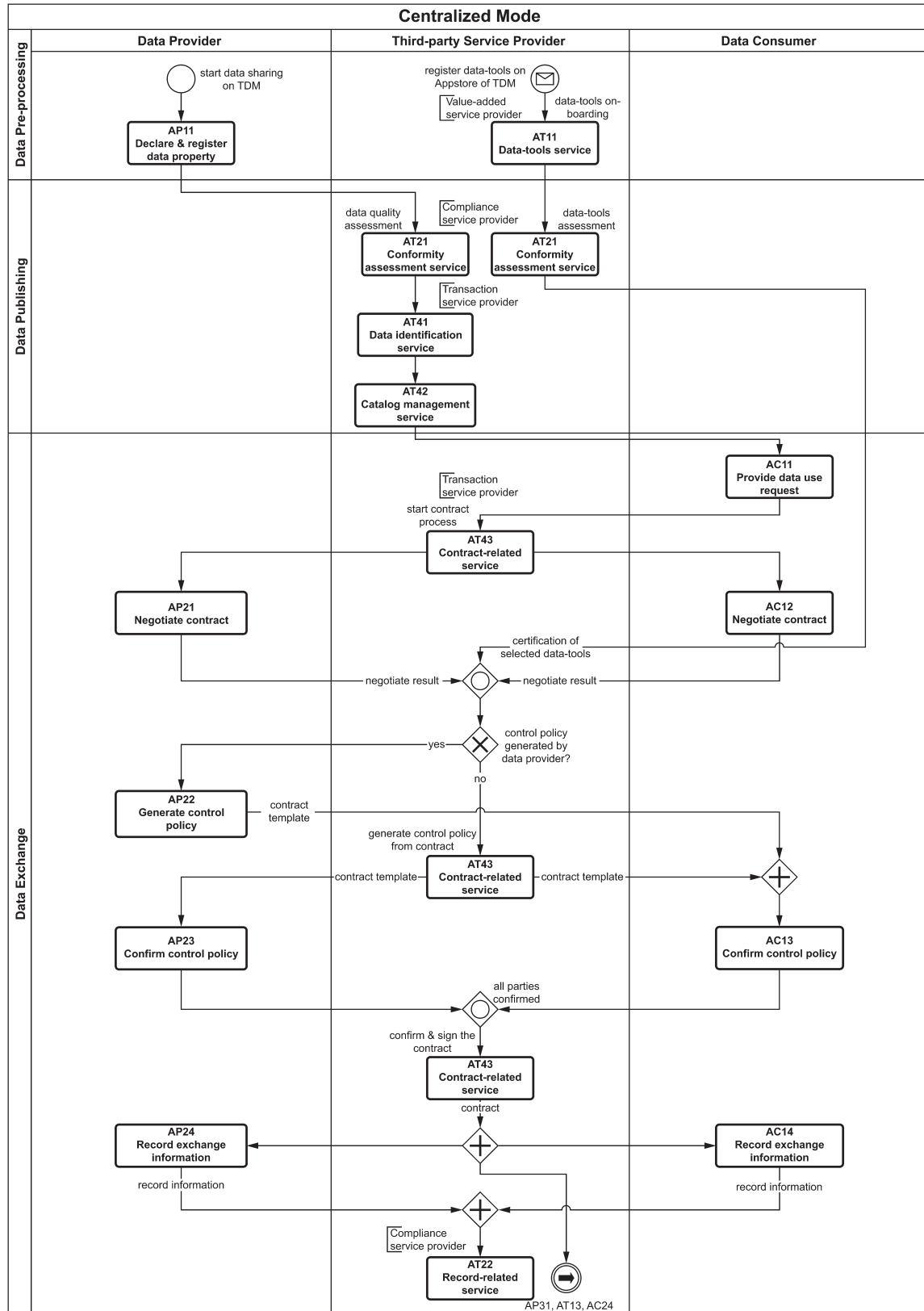


Figure 7—Working flow of pre-processing, data publishing, and data exchange stages

In the data pre-processing stage, the data provider declares and registers the data set that requires for sharing as own property. The value-added service provider applies to register their data-tools on the APP store of TDM in the data-tools on-boarding.

In the data publishing stage, the data provider should confirm the quality of their data resources or provide the certification by compliance service provider, such as the professional testing of institutions and laboratories. After that, the data provider applies a global unique identifier from transaction service provider, which is allocation to mark the data property. The identifier and metadata information would be enrolled by transaction service provider, and the data catalog is maintained and updated for stakeholders to prepare the data exchange business. In addition, before the on-boarding of a data tool, its performance and security need to be certified by APP store.

In the data exchange stage, the data consumer searches the data catalog and submits a data use request to initiate a data sharing or data exchange transaction. The transaction service provider can also provide a data use requirement list for data providers to understand the demands if there is no required data in the data catalog. Through contract-related service by third-party service providers, data consumer and data provider negotiate the contract, choose the data-tools, and agree the control policy. The control policy could be generated by the data provider or negotiated result from contract and should be confirmed by all stakeholders. The data consumer and data provider could sign the contract offline or sign it online by digital signatures. The data consumer and data provider record the contract and other information of data exchange activities. The contract would be distributed and executed by data provider, data consumer, and third-party service providers.

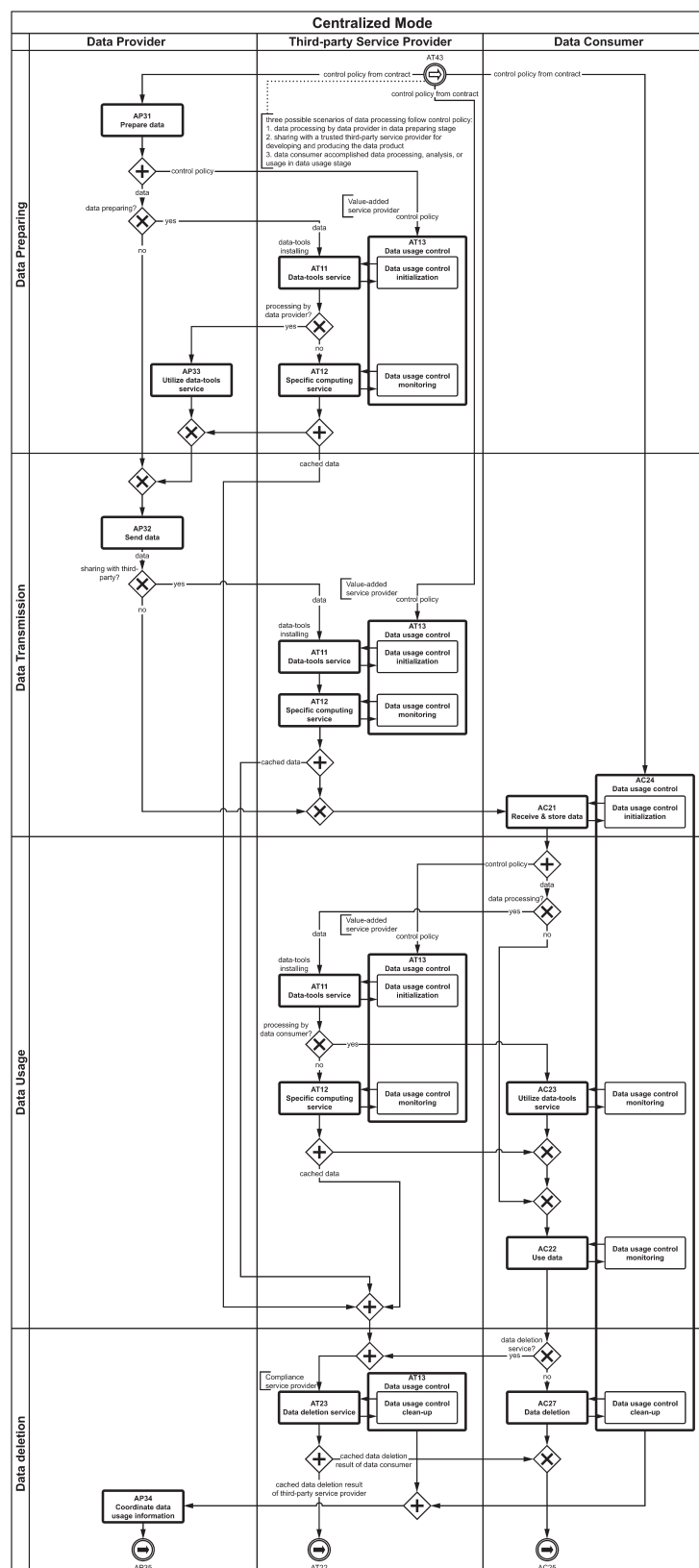


Figure 8—Working flow of data preparing, data transmission, data usage, and data deletion stages