INTERNATIONAL STANDARD

# ISO/IEC 24039

First edition
2022-06

# Information technology — Smart city digital platform reference architecture — Data and service



Reference number
ISO/IEC 24039:2022(E)



ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

# Contents

Page

# Foreword

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

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see https://patents.iec.ch).

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

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

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

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

# Introduction

Smart city digital platforms (SCDPs) aim to form a pragmatic development of information technology foundations that enable the integration of urban services. SCDPs are part of the digital transformation in urban infrastructure and services that is being driven by the deployment of the internet of things (IoT), artificial intelligence (AI), cloud computing, big data and digital twin solutions, and other digital technologies.

An SCDP is a space where different applications can share fundamental common resources and functions. It provides an interface to integrate a city's digital and physical infrastructure. It also provides integrated capability to coordinate data, services and applications across operational domains for multiple stakeholders in smart cities.

An SCDP is intended to help to break down the traditional system silos of a city by bringing connections between them. It looks beyond sectoral silos to reimagine existing systems, enable new processes and interactions, and migrate towards new forms of service delivery. The digital capabilities provided by SCDPs aim at connecting things, connecting data and connecting innovation. These capabilities are key criteria for enabling cities to build partnerships to ensure their economies, environment and services are fit for the future.

# Information technology — Smart city digital platform reference architecture — Data and service

## 1 Scope

This document specifies the reference architecture of smart city digital platforms (SCDPs), with a focus on supporting access to data and services for applications in smart cities.

## 2 Normative references

There are no normative references in this document.

## 3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

**3.1**
**asset**
anything that has value to a stakeholder

[SOURCE: ISO 22739:2020, 3.1]

**3.2**
**data**
representation of facts of objective reality in a formalized manner

EXAMPLE Data can be signs and symbols, and can be in analogue form, digital form or both.

Note 1 to entry: Data can be used for communication, interpretation or processing by human beings or automatic means.

[SOURCE: IEC CDV 60050-831, 2.2]

**3.3**
**information**
structured, contextualized and processed data that are endowed with meaning

Note 1 to entry: Information is meaningful and useful to human beings, or machines or both.

**3.4**
**interoperability**
property permitting diverse systems or components to work together for a specified purpose

[SOURCE: IEC 80001-1:2010, 2.11]

**3.5**
**metadata**
data about data or data elements, possibly including their data descriptions, and data about data ownership, access paths, access rights and data volatility

Note 1 to entry: The term "metadata" in this document mainly aims to aid the identification, discovery, assessment and management of the data collected by SCDP.

[SOURCE: ISO/IEC 20546:2019, 3.1.24, modified — Note 1 to entry is added.]

**3.6**
**platform**
combination of an operating system and hardware that makes up the operating environment in which a program runs

[SOURCE: ISO/IEC/IEEE 26513:2017, 3.30]

**3.7**
**smart city digital platform**
**SCDP**
combination of software and hardware that makes up the operating environment to support smart city common services and applications

Note 1 to entry: The operating environment enables data from a variety of sources to be processed and common services to be provided.

Note 2 to entry: Common services are aimed at improving the interoperability of cross-domain systems, for example data exchange, catalogue service, subscription and distribution, etc.

## 4 Overview

A SCDP connects smart city information and communication technology (ICT) infrastructure, such as device, network and Internet, and smart city applications, such as e-government and public service, city operation, decision-making and industry service, as shown in Figure 1. The SCDP is characterized by the combined exploitation of software components with heterogeneous physical devices and protocols, furnishing smart city applications with ready-to-use software services and enhancing the system performance in various system environments. This ultimately provides optimized and integrated city services to the end users, such as governments, individuals, organizations and companies. One example of SCDP data service reusability for different applications is provided in Annex A.

SCDPs implement capabilities of the data and services supporting layer described in ISO/IEC 30145-3 (see Annex B). Guided by the design principles in Clause 5, the functions of an SCDP can be categorized into four groups:

1) technical support,
2) resource management,
3) capability exposure, and
4) interface.

This is shown in Figure 1.

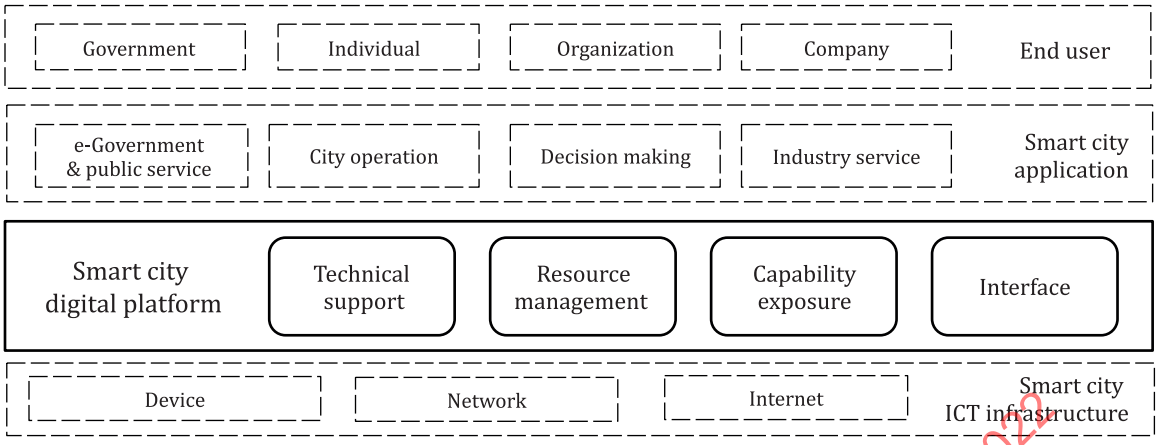



**Figure 1 — Functions of a smart city digital platform**

**Technical support**: aims at providing reliable and scalable technical and system tools to help improve data integration and service aggregation and to build horizontal foundations to eliminate information silos.

**Resource management**: aims at guaranteeing migration of resources, transparency of processes, quality of data and services, operation efficiency and service evolution.

**Capability exposure**: aims at enabling reuse and openness, integrating business value with data and services and providing ready-to-use functional blocks for smart city applications.

**Interface:** aims at providing a unified approach to access interfaces to reduce process complexity for external access and enable flexible interactions.

## 5 Design principles

The design principles of SCDPs are as follows:

**Holistic**: looking beyond information silos to reimagine existing systems, create new processes and interactions, and migrate towards new forms of service delivery, in order to avoid information silos and to generate interoperable, standards-based, replicable and scalable solutions for cities.

**Modularity**: utilize advantages of service-oriented architecture and microservice architecture, provide loosely-coupled service modules which support the constant evolution of robust and powerful services and flexible adaptation to various new business requirements;

**Transparency**: data and services should be able to exchange, process and deposit with standard format and trackable flow. This improves the interoperability and transparency of the platform in order to improve operational efficiency and value creation for cities;

**Reusability**: data, services and applications need to be utilized based on shared capabilities and functionality, in order to fulfil rapid response requirements for new businesses and avoid repetitive development investment;

**Security**: data, services and applications need to be secure by design.

Table 1 shows the linkage between design principles and the SCDP function groups.

**Table 1 — Function group mapping with design principal**

| | Holistic | Modularity | Transparency | Reusability | Security |
|---|---|---|---|---|---|
| Technical supporting | X | X | X | X | X |
| Resource management | X | X | X | X | X |
| Capability exposure | | X | X | X | X |
| Interface | | | X | X | X |

## 6 Reference architecture

The reference architecture from the functional viewpoint of SCDPs with a focus on supporting external access of data and services is shown in Figure 2.

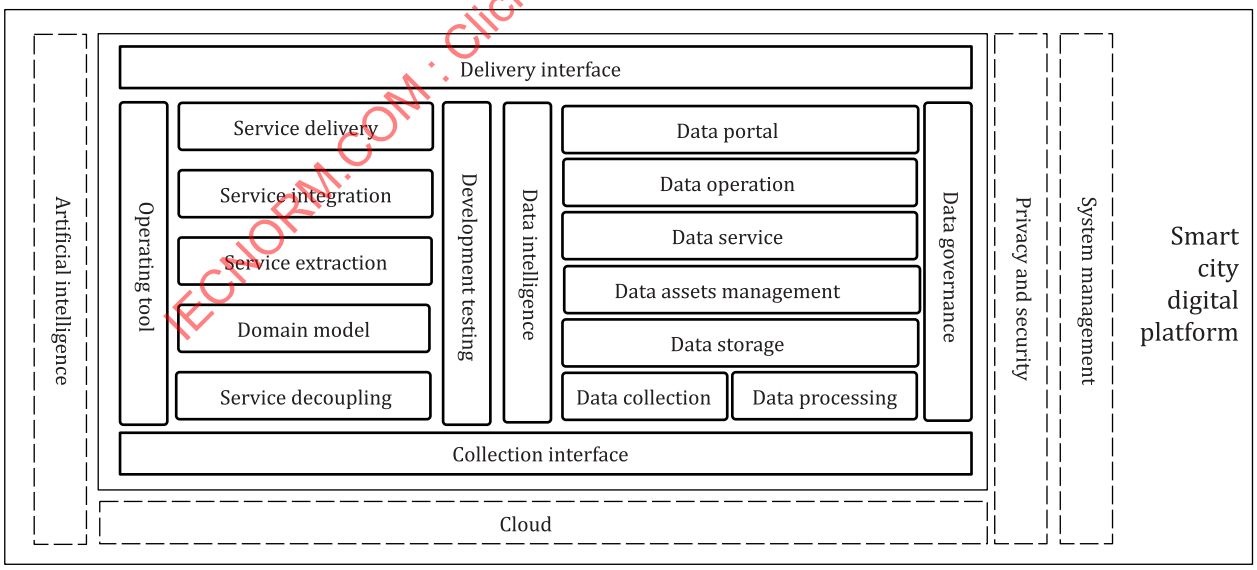
The technical support function group as described in Clause 4 and Figure 1 includes functions of data collection, data processing, data storage, operating tools and development testing.

The resource management function group as described in Clause 4 and Figure 1 includes functions of data assets management, data governance, data intelligence, service decoupling, domain model and service extraction.

The capability exposure function group as described in Clause 4 and Figure 1 includes functions of data service, data operation, data portal, service integration and service delivery.

The interface function group as described in Clause 4 and Figure 1 includes functions of collection interface and delivery interface.

NOTE Functions shown in dotted line blocks including artificial intelligence, cloud, privacy and security and system management in Figure 2 are not included in this document.




NOTE Within Figure 2, a special focus is placed on supporting external access of data and services.

**Figure 2 — Reference architecture from the functional viewpoint of smart city digital platforms (SCDPs)**

**Data collection** is a process for the collection of qualitative and quantitative data via digital tools or software from various sources.

**Data processing** is the manipulation of data to produce meaningful information and insight.

**Data storage** is the collection and retention of digital information in a storage medium.

**Data asset management** refers to the software components which establish a systematic approach to organizing and retrieving the assets.

**Data governance** is a process focused on managing the quality, consistency, usability, security and availability of data.

**Data intelligence** is the process of using artificial intelligence (AI) and machine learning tools to analyse and transform massive data sets into intelligent data insights, which can then be used to improve services.

**Data service** refers to software services that encapsulate operations on key data entities of relevance to stakeholders.

**Data operation** is a process to create business value from data with a systematic data management methodology.

**Data portal** is a system or platform which supports users in accessing collections of data.

**Service decoupling** is a process of segregating service flows into independent functional modules.

**Domain model** is a conceptual model of the domain that incorporates both behaviour and data.

**Service extraction** is a process of selecting and orchestrating necessary service modules to meet specific requirements.

**Service integration** is a process of integrating interdependent services from various internal and external service modules into ready-to-use services in order to meet specific requirements.

**Service delivery** is a process of enabling users to access and receive required services.

**Operating tool** is a set of foundational functions for effective running of hardware and software.

**Development testing** is a software development process that involves the synchronized application of a broad spectrum of defect prevention and detection strategies in order to reduce software development risks, time and costs.

**Collection interface** is the interface where an SCDP collects data from external hardware infrastructure and software systems.

**Delivery interface** is the interface where an SCDP provides services or capabilities for external systems or users.



# 7 Technical support

## 7.1 Data collection

Data collection capabilities provided by an SCDP should:

a) support the collection of structured data, semi-structured data and non-structured data;

b) support the collection of bulk data, near real-time data and real-time data;

c) support unified data collection management, such as management of data source, acquisition frequency, acquisition range, etc.;

d) support data import, data export and data exchange with external data sources, such as relational databases, file servers, etc.;

e) support various data collection methods, such as automatic collection, manual report, file upload, interface call, etc.

## 7.2 Data processing

Data processing capabilities provided by an SCDP should:

a) support the extraction of data in real time or at regular intervals according to customized requirements;

b) support distributed data processing, bulk data processing and real-time streaming data processing;

c) support various mainstream data processing frameworks, such as batch processing, interactive queries, data retrieval, real-time streaming, memory computing, etc.;

d) support mainstream data processing operations, such as task creation, orchestration, execution, monitoring, etc.;

e) enable extract-transform-load (ETL) capabilities, such as data extraction, cleaning, conversion and loading;

NOTE ETL is used to extract necessary data from data sources such as databases, to transform the data into the desired form, and to load them into a target system.

f) support data semantic capability by supporting data re-organization according to a city data model;

g) provide data processing visualization via a componentized toolbox or other methods;

h) enable data format conversion, enrich data by merging data from multiple sources, perform aggregation functions, i.e. create summary of data, or cleanse data with null values;

i) enable data packing and compression with a pre-defined data format before the data has been transmitted, and only transmit the packed and compressed data;

j) ensure the pre-defined data format includes special field, creation-time field, sub-package field, and the number of sub-package fields. Each sub-package field should include a property field and frame field. The frame field should include frame-length field, frame-compression field and frame-payload field.

## 7.3 Data storage

Data storage capabilities provided by an SCDP should:

a) enable massive data storage capabilities, such as building a distributed storage system on top of a distributed file system;

b) support a distributed relational database, which is able to manage a petabyte of data storage;

c) support a data warehouse or data lake, such as those providing structured data storage services and basic data analysis services;

d) support line storage, column storage, key-value storage, row-organized tables and column-organized tables;

e) support file storage and basic operations for file systems, such as file upload, file download, directory view, directory creation, directory deletion, file permission modification, etc.;

f) support conversion of data between different storage dimensions;

g) support multi-tenancy, resource isolation and customized configuration;

h) support different storage options for hot data, warm data and cold data;

i) enable protocol conversion with a common data protocol to identify data task property information, interface information and time property information;

j) enable distributed data storage according to task property information of the received data;

k) ensure all data sent to the distributed file system for storage has been pre-processed and sorted.

## 7.4 Development and testing

Development and testing capabilities provided by an SCDP should:

a) provide software development tools for application programming interfaces (APIs), microservices, software as a service (SaaS) development, data modelling, visual design, etc.;

b) be compatible with architecture models such as client/server and browser/server;

c) provide packaged computing environment capabilities, such as container and virtual machine (VM);

d) provide caching mechanisms to improve application performance;

e) enable connection for different functions, software modules and systems, such as terminal emulation, data access, remote procedure, message, transaction, etc.;

f) support large-scale parallel processing and testing by supporting cluster-based architecture with non-shared resources, fully symmetric and distributed multi-nodes;

g) ensure there is no single point failure in system design.

## 7.5 Operating tool

### 7.5.1 Life cycle management

Life cycle management capabilities provided by an SCDP should:

a) enable service registration capability to ensure that only authorized users can add new services into the service catalogue;

b) enable service review and service release mechanisms to support authorized users in updating the service catalogue;

c) enable service audition before releasing the registered services to the public or specific departments, roles, or users based on access control requirements;

d) enable the start/stop capability for the system administrator or advanced authorized users to manually control the start-up status of the service which is open to external use;

e) enable the service logout capability to dismiss services that are no longer valid. Users subscribed to the dismissed services should receive a notification, and the dismissed services cannot be accessed via the service catalogue.

### 7.5.2 System operation

System operation capabilities provided by an SCDP should:

a) enable seamless connection capability between distributed relational databases, traditional relational databases, data warehouses and other types of data storage options;

b) support automatic failure detections and process database switching when part of the database fails, in order to ensure continuity of services;

c) enable full-text search, query and row-organized table association query;

d) enable catalogue and basic information management capabilities for service management nodes of the platform, including but not limited to registration, logout and global parameter configuration;

e) support service management capabilities in distributed and coordinated manners. It should maintain synchronization and ensure consistency for data, heartbeat, time and other system performance indicators among management nodes;

f) enable identification capability for service management nodes to avoid malicious attacks from third parties;

g) enable access authentication for services and related information. Service and related information can be accessed by searching the service catalogue or subscribing to interested service portfolios;

h) support service usage monitoring, such as running status, successful access rate, access statistics, access time distribution and access logs;

e) enable automatic alert for abnormal system conditions, and automatic trigger service recovery via SMS, email, system messages and other methods;

j) enable periodic evaluation and testing of system security.

# 8 Resource management

## 8.1 Data governance

### 8.1.1 Data ownership identification

Data ownership identification capabilities provided by an SCDP should:

a) define the ownership of the source of original data resources, define the ownership of stakeholders or parties involved in data collecting and processing, such as data conversion, data cleaning, data modelling and data analysing.

If the ownership of data assets involves multiple stakeholders or parties, it should define respective proportion, scope, limitations, etc. for each stakeholder or party.

The data ownership information should be assigned with a unified identifier. The ownership information should be able to be requested and updated via the identifier.

### 8.1.2 Metadata management

Metadata management capabilities provided by an SCDP should:

a) support metadata persistent storage, metadata model creation and maintenance, maintenance update, query retrieval and version control of metadata content;

b) enable a management system for metadata to ensure the integrity, uniqueness, consistency, accuracy, legality and timeliness of collected data;

c) maintain multiple copies of the metadata. The capabilities of automatic detection and recovery are required if one of the copies is lost or damaged;

d) enable basic operations for metadata, such as addition, deletion, modification and investigation;

e) provide life cycle management for metadata and enable users to develop data management strategies, processes and activities;

f) enable users to manage and control metadata creation, reception, distribution, use and destruction.

### 8.1.3 Data quality

Data quality capabilities provided by an SCDP should:

a) support data quality monitoring and control mechanisms;

b) ensure data sources are checked in terms of data format, value range, duplicated data and data integrity and accuracy;

c) provide data quality control, including but not be limited to: quality rule management, quality model, quality inspection check, quality monitoring, etc:

NOTE Quality rule management refers to the definition, modification and deletion of quality rules; quality model configures, modifies and deletes quality rules for data items in a data catalogue; quality inspection check configures tasks for data catalogue and data quality periodically; quality monitoring includes but is not limited to: data quality report, quality problem distribution, data quality trend analysis and data quality statistics.

### 8.1.4 Data policy

The data policy capabilities provided by an SCDP should:

a) trigger accessibility updates for data and data sets;

b) enable frequent and regular evaluation of the intended use of data and purpose for which the data are collected, created, stored, used, processed, disclosed or disseminated;

c) enable a data protection policy to ensure fair use of data related to people, such as proper and responsible collection, creation, use, processing, sharing, transfer, disclosure, storage, security, retention and disposal of information about people;

d) enable privacy protection mechanisms for data that can potentially be linked to personal information, such as home address, communication records, opinions, beliefs and identities;

e) enable user-customizable data policy creation and management;

f) enable data categorization to ensure efficient and effective use in line with local data policy and standards.

## 8.2 Data assets management

### 8.2.1 Data asset identification and registration

Data asset identification and registration capabilities provided by an SCDP should:

a) support data asset classification and provide guidance on how to classify data assets;

b) support extension of existing data asset types;

c) assign unique asset identifiers within a certain boundary so that data assets can be correctly found and accessed;

d) support different asset identifier methods, such as literal identifiers, synthetic identifiers, relationship identifiers, etc;

e) support data asset registration for each data asset that can be accessed by a third party;

f) maintain a list or inventory for all registered data assets.

### 8.2.2 Data asset directory and catalogue management

Data asset directory and catalogue management capabilities provided by an SCDP should:

a) enable data asset catalogue classification and management according to different applications from the perspective of category name, category coding, etc.;

b) enable data asset directory management, including metadata management, directory preparation, directory publishing and directory information maintenance, according to the content of data combined with other relevant requirements to form a data directory;

c) enable dynamic management of the data asset directory and support dynamic requirement-based directory adjustment.

### 8.2.3 Data asset model

The data asset model capabilities provided by an SCDP should:

a) support a customized data asset model based on business needs and metadata information;

a) enable the capability of applying mature data modelling techniques to build data asset models for smart city applications;

b) enable the capabilities of determining data and associated processes, defining data, verifying the integrity of data, defining operational procedures, and selecting data storage technologies;

c) enable the capabilities of building conceptual modelling, logical modelling and physical modelling;

d) enable the capabilities of supporting data modelling with hierarchical models, mesh models and relational models.

### 8.2.4 Data asset association

Data asset association capabilities provided by an SCDP should:

a) support searches for frequent patterns, associations, correlations or causal structures among data;

b) provide the capability of identifying static data associations and dynamic data associations;

c) provide the capability of identifying associations of data catalogues with technical metadata;

d) provide the capability of correlation and fusion between different data sets by various technical means and correlation algorithms;

e) provide the ontology used in the data set when the linked data are published.

### 8.2.5 Data asset security

Data asset security capabilities provided by an SCDP should:

a) enable cloud-native security controls for data and service throughout the whole lifecycle, including key management service (KMS), credential management system (CMS) and cloud hardware security module (HSM);

b) implement the principle of least privilege (PoLP), also known as the principle of minimal privilege or the principle of least authority, so that each functional entity accesses only the information and resources that are necessary for its legitimate purpose;

c) prevent unauthorized access for individual and non-personal entities, in order to reduce the exposure of digital assets;

d) provide audit and accountability mechanisms to ensure conformance and track authorized changes;

e) enable transport layer security (TLS) 1,1 or higher transport layer encryption;

f) enable two-step authentication for functionalities or platform modules which process or are related to sensitive data;

g) enable selective restriction of data access based on classification of data or authorization level of access entity;

h) have data access control to protect data from unauthorized access and data corruption throughout its lifecycle;

i) provide the capability of protecting sensitive data by technologies such as data encryption, masking, hashing and tokenization;

j) provide the capability of monitoring data activities to detect anomalies and identify risks;

k) ensure that lost data can be recovered in the event of unexpected disruptive events or hardware failures;

l) provide capability to completely erase data on all storage devices to ensure that it is unrecoverable.

## 8.3 Data intelligence

### 8.3.1 Data training

Data training capabilities provided by an SCDP should:

a) support various built-in data training algorithms;

b) enable training model import, creation and management;

c) support distributed training with containers;

d) support various learning methods including supervised learning, unsupervised learning, semi-supervised learning and reinforcement learning;

e) provide capability of avoiding overfitting and bias;

f) support training performance evaluation including but not limited to precision, recall, sensitivity and specificity;

g) support incremental data learning to adapt to new data;

h) support multi-source data training;

i) support both online and offline data training.

### 8.3.2 Data analysis

Data analysis capabilities provided by an SCDP should:

a) support automatic data analysis and integration from multiple sources to accomplish the required decision-making and estimation tasks;

b) support functions such as data association, estimation and identification;

c) provide various capabilities for data analysis, including but not limited to descriptive analysis, diagnostic analysis, predictive analysis, causal analysis, support of trusted environment, etc.;

d) support big data analysis capabilities, including analytic visualization, data mining algorithms, predictive analytic capabilities, semantic engines, data quality and master data management;

e) provide multiple data analysis modes, such as offline analysis, real-time analysis, interactive analysis, etc.;

f) support various data analysis models, algorithms and tools, such as statistical analysis, machine learning, text analysis, video analysis, etc.;

g) support orchestration of the data analysis process;

h) provide capability of identifying and correlating for requirements of specific scenario and data analysis methods.

#### 8.3.3 Data visualization

Data visualization capabilities provided by an SCDP should:

a) enable the visualization of data, algorithms, tools and system components;

b) support revealing of data relationships, features, or trends via various methods, such as interactive tables, highlight tables, histograms, box plots, reporting tools, business intelligence (BI) tools, etc.;

c) enable accessibility management for visualization results and provide multiple download formats.

### 8.4 Service decoupling

Service decoupling capabilities provided by an SCDP should:

a) enable service decoupling capability to formalize native atom service repository and microservices. The service decoupling can be based on time, connection, process and business logic;

b) support asynchronous service invocation for reducing temporal coupling;

c) standardize service agreements for communicating with services;

d) support stateless connections to services without state data;

e) enable the capability of connecting services without knowing where the services are located;

f) ensure that services are self-contained;

g) minimize the dependency between services;

h) ensure that services can be evolved without impacting other services.

### 8.5 Domain model

#### 8.5.1 Domain knowledge

Domain knowledge capabilities provided by an SCDP should:

a) enable the capability of representing specific knowledge for various domains;

b) enable the capability of capturing domain environment, configurations and constraints.

#### 8.5.2 Domain business logic

Domain business logic capabilities provided by an SCDP should:

a) enable capability of modelling business logic for various domains;

b) support business logic isolation for limiting the impact caused by business logic changes.

### 8.6 Service extraction

Service extraction capabilities provided by an SCDP should:

a) enable capability of supporting hierarchical catalogue structure;

b) enable capability of supporting unified service catalogue display.

## 9 Capability exposure

### 9.1 Data service

Data service delivered by an SCDP should:

a) enable capability of providing tool-based data service, content-based data service and API-based data service for users to subscribe;

NOTE Tool-based data service refers to data services which can be used as tools for further data processing. Content-based data service refers to data services which aim to deliver data or data sets. API-based data service refers to data services which are delivered via API.

b) support configuration and customization of the tools according to users' settings;

c) support users in integrating with their internal systems;

d) ensure content-based service is delivered to consumers with a predefined standard format;

e) inform consumers with metadata definitions;

f) support managing API-based services such as monitoring usage, analysing statistics and enforcing usage policies;

g) support publishing API documentations describing the purpose, functionality, inputs and outputs for each API.

### 9.2 Data operation

#### 9.2.1 Authorization

Authorization capabilities provided by an SCDP should:

a) enable data rights registration, confirmation, rights verification and tracking;

b) enable data rights authorization, such as data ownership rights, data management rights, data usage rights, data processing rights, data awareness rights, data privacy rights, etc.;

c) confirm rights authorization before providing data and services to third parties. The service provider should perform data and service authorization confirmation for requests to access non-public information of individuals or enterprises;

d) enable functional configuration control with multi-level, multi-role structure;

e) enable scalability and stability authorization management capability to support a large number of user authorizations;

f) enable various authorization methods, such as counter-authorization, self-authorization and remote-authorization.

#### 9.2.2 Circulation

Circulation capabilities provided by an SCDP should:

a) enable share, open, exchange, trade, engage and other circulation methods for data and services;

b) enable collect data and service requirements, process, distribute and release data and services;

c) support online trading for available data, services and other types of resources.

### 9.3 Data portal

Data portal capabilities provided by an SCDP should:

a) enable data and data sets search, upload, download and interaction via portal;

b) ensure data searching meets user-specified criteria;

c) support data searching with Boolean operators such as AND, OR and NOT;

d) enable the capability of refining search results including filtering and weighting;

e) support real-time searching;

f) support uploading data in various file formats;

g) support different metadata upload, including descriptive metadata, structural metadata, administrative metadata, reference metadata and statistical metadata;

h) support downloading data in various formats;

i) support refining data to be downloaded including horizontal and vertical filtering;

j) support splitting large volumes of data into multiple files with specified file size limit;

k) enable classified display capabilities with unified interfaces;

l) enable data legality verification, flow record, black and white list management, authentication, charging, daily maximum access control, access failure record, flexible reverse proxy and dynamic routing.

### 9.4 Service integration

#### 9.4.1 Service interaction

Service interaction capabilities provided by an SCDP should:

a) enable capabilities of service identification and service component communication, to ensure interconnection, communication, load balancing and interaction message delivery among services;

b) enable protocol conversion to ensure the matching of specifications and standards required for information exchange of services, and to improve compatibility between heterogeneous services;

c) enable capability to trigger the service with scheduled start or event start;

d) enable service process orchestration to support logic-based service combination and support semantic handling for order, condition, loop, exception, etc.

#### 9.4.2 Service encapsulation

Service encapsulation capabilities provided by an SCDP should:

a) be developer-oriented and ready to use. They should not introduce further complicated software developments;

b) be manageable according to corresponding user authorities, unless published as open services;

c) restrict direct access and provide publicly accessible methods to access the service components;

d) support hiding unnecessary details about the services, such as the internal logic and mechanisms, to limit the dependency between services;

e) ensure the underlying technologies used within the service are transparent to the consumers.

### 9.5 Service delivery

#### 9.5.1 Service accessibility

Service accessibility capabilities provided by an SCDP should:

a) enable unified management for service registration, authorization, operational status search and configuration;

b) enable user confirmation to ensure services are accessed by users with valid authority.

#### 9.5.2 Delivery management

Delivery management capabilities provided by an SCDP should:

a) enable unified lifecycle delivery management, including access management, interface management, version management, classification management, hierarchical management and quality management;

b) enable unified operation status management, such as service monitoring, service log management, etc.;

c) enable service isolation and circuit break capabilities;

d) enable service process orchestration and routing capability, as well as enabling semantic capability for handling order, condition, loop and exception;

e) enable at least one of the delivery methods such as API gateway, micro-service gateway, SaaS service gateway, etc.;

f) enable routing selection capability, including but not limited to point-to-point, publish and subscribe, content-based routing and other routing methods.

#### 9.5.3 Service evaluation

Service evaluation capabilities provided by an SCDP should:

a) enable service audit capabilities, such as service access and traffic, data download and record, event logs, etc.;

b) provide service audit summary, query and backup of the audited information;

c) enable service impact assessment based on dependencies among services, and evaluate impact of service changes and decommissioning on other services;

d) support service failure root diagnosis based on the service audit record.

# 10 Interface

## 10.1 Collection interface

### 10.1.1 Secure access

Secure access capabilities provided by an SCDP should:

a) ensure secure connections within SCDP components and external systems;

b) support authentication and authorization before connecting with cloud or ICT infrastructures;

c) provide task identification information, task property information, data source information, interface information and store information, at least for access configuration;

d) collect real time data at least once from the configurated data sources as listed in the task identification information.

### 10.1.2 Digital representation

Digital representation capabilities provided by an SCDP should:

a) support digital representation for all connected source of data and service;

b) support 3D representation for all physical objects in cities, such as buildings, roads, public facilities, etc.;

c) perform connection and access configuration before digital representation and physical objects are linked with each other.

### 10.1.3 Command distribution

Command distribution capabilities provided by an SCDP should:

a) support sending real-time control commands to devices and ICT infrastructures connected to SCDP;

b) ensure messages and commands send to applications, devices and ICT infrastructures with specific customize formats.

### 10.1.4 Message push

Message push capabilities provided by an SCDP should:

a) enable message push subscribed by the connected resources, devices and ICT infrastructures;

b) provide change notification for subscribed information so that the subscribed devices and ICT infrastructures perform corresponding actions.

### 10.1.5 Service access

Service access capabilities provided by an SCDP should:

a) support a task scheduling interface for accessing services by third-party platforms or systems;

b) support high-throughput data access capabilities, such as supporting large-scale data integration applications, fast retrieval of data stored in distributed file systems, and provision of interactive queries.

### 10.1.6 Protocol and format translation

Protocol and format translation capabilities provided by an SCDP should:

a) enable translation of internal service and data formats for external platform compatibility and consumption;

b) enable protocol translation for external platform compatibility and consumption, for example simple object access protocol (SOAP) to representational state transfer (REST).

## 10.2 Delivery interface

### 10.2.1 Authentication

An SCDP should provide authentication via an interface or other methods before application to access data and services.

### 10.2.2 Inquire

An SCDP should support inquiry via an interface to discover available data and services, perform statistical analysis, etc.

### 10.2.3 Subscription

Subscription capabilities provided by an SCDP should:

a) support subscription management, such as creating subscription, renewing subscription and unsubscribing;

b) support subscribers in confirming their subscriptions;

c) support subscribers in selecting which services they would like to manage, and support subscribers in updating their email address, organization name and contact details;

d) support applications in the subscription of data and services and manage subscriptions via an interface.

### 10.2.4 Procedure call

Procedure calls capability should enable valid applications to configure, deactivate and use services of an SCDP via an interface or other methods.

### 10.2.5 System call

An SCDP should:

a) support interface or other methods for applications in making system calls to manage and maintain processes, files and devices;

b) support interfaces for applications to query, schedule and manage system calls.

### 10.2.6 Application programming interface (API)

An SCDP should:

a) enable API management for applications to query, schedule and manage the applications connected with an SCDP;

b) enable capability of common communication protocol adaptation and conversion via an API.

# Annex A
(informative)

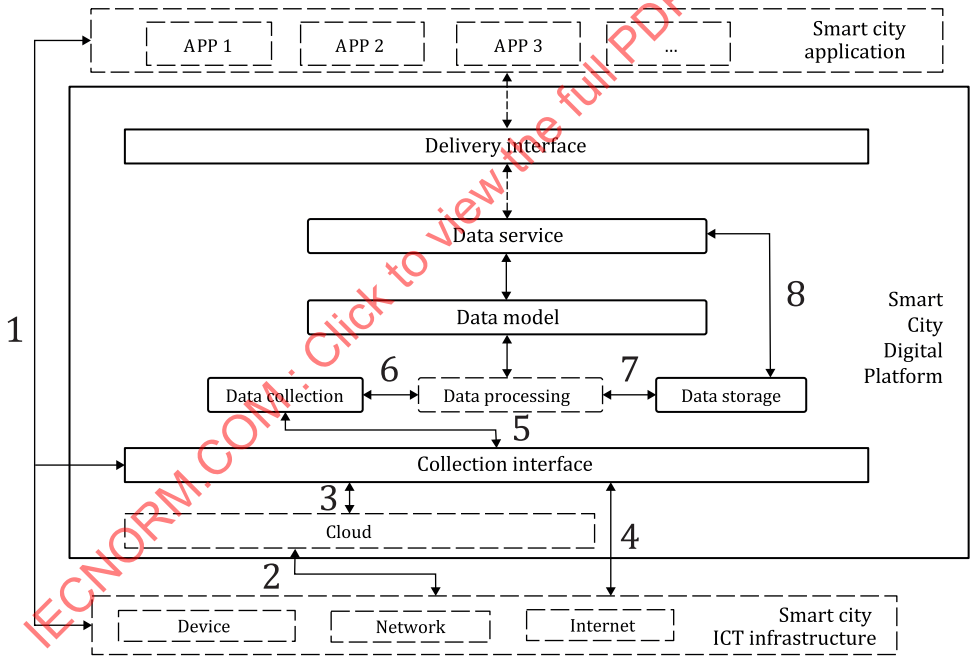
# Example of SCDP data service reusability

In this example, an SCDP is taken to provide ready-to-use and reusable services to improve platform operation and service response efficiency.

On one hand, the SCDP generates a reusable data service with collected data based on a data model, shown as solid arrows in Figure A.1. Smart city ICT infrastructure can collect and exchange data and information generated by smart city applications (see label 1 in Figure A.1). The data and information collected by smart city ICT infrastructure can also be stored or processed via the cloud to the SCDP collection interface (see label 2 in Figure A.1). Thus, different extraction or acquisition tools, including using ETL tools, are required to directly extract data from the relevant database. The data collection provided by the SCDP via the collection interface enables applications to push related data and information (see labels 3-5 in Figure A.1).

Once a set of data and information is collected by the SCDP, it will be processed in accordance with the relevant standard data model before being stored in the SCDP. It will then be formalized or encapsulated as a certain type data service (see labels 6-8 in Figure A.1).






NOTE The data model component in Figure A.1 contains a set of standard data models which are abstracted from different scenarios. The standard data model for a specific scenario is applied for any applications for that scenario.

**Figure A.1 — Data service reusability of SCDP**

On the other hand, a smart city application initiates a data service request to the SCDP, shown as dotted arrows in Figure A.1. The data request via the delivery interface of the SCDP contains the requested data type, field list, data time interval, record number and other parameters used to clarify the data request.

After the SCDP receives the request, it will complete an internal search of registered data services and data storage to identify the data set that meets all requirements of the data request, then formalize or