ISO/TC 268/SC 1
Smart community infrastructures

Email of secretary: chiba@jsa.or.jp
Secretariat: JISC (Japan)

ISO CD 37156 for ballot

Document type:	CD ballot
Date of document:	2018-06-29
Expected action:	INFO
Background:	Dear members of ISO/TC268/SC1 The CD ballot for ISO 37156 (SC1/WG4) will be started from 2nd of July for 8 weeks. Please cast your national vote via eBalloting Portal.
Committee URL:	https://isotc.iso.org/livelink/livelink/open/tc268sc1

ISO 37156:2018

ISO TC 268/SC 1

Secretariat: JISC

Date:2018-07-02

Guidelines on Data Exchange and Sharing for Smart Community Infrastructures

CD stage

Warning for CD

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Contents

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO 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).

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

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 268, Sustainable cities and communities], Subcommittee SC 1, Smart community infrastructures.

Introduction

Community is the crystallization of human technological progress, economic development and social civilization. It is also the basic unit of human economic activities and regional production. Community function and people's daily life are highly dependent on different types of community infrastructure. As the foundation of survival and development, community infrastructure includes energy, water, transportation, waste, information, communication technology and so on. The community infrastructure provides convenience for urban residents. Therefore, the scientific and effective management of community infrastructure is crucial. It will affect living quality of citizens, efficiency of social economy and ecological safety of community. Poor management of community infrastructure will cause problems such as environmental pollution, traffic congestion, inadequate urban resources and weak urban lifeline system. It is unfavorable for the sustainable development.

Data is the fundamental basis of effective management. It is a common problem that different organizations or departments govern data of community infrastructure. The information silos among them affect the efficiency of management. Therefore, strengthening the sharing of data is an important aspect of the smart community. Standardized data sharing and exchange will benefit business collaboration across departments. It will also improve the services' capabilities of community infrastructure. What is more, it will make the management of community more scientific, and the community will be safer hospitable and livable.

This document is a reference for governments and other enterprises, organizations, and individuals who have the responsibility or need to share data on community infrastructure. This document helps to promote a baseline of information, eliminate isolated information islands, and move toward more smartness. As one example of this, the document promotes efficient cooperation by establishing mechanisms for information exchange among different departments within local governments.

This document provides a set of community infrastructure data organizing methods and a unified framework of community infrastructure data exchanging, sharing and security. The purposes of this document are:

— Providing intensive, efficient, convenient, ecological and secure infrastructure for community infrastructure users, consumers or beneficiaries.

— Providing appropriate approaches to exchange, sharing and maintenance of community infrastructure services.

— providing a digital continuity framework for the sustainable community infrastructure data sharing and exchange platform provider, which enables better connectivity of products, services and solutions.

This document is about smart community infrastructures, as well as ISO 37101, ISO 37120, ISO37150, ISO 37151. The ISO 37101 is requirements of different types of data supporting. The ISO 37120 provides macro-guidance to cities on how to achieve sustainable development goal. Under the macro-guidance from ISO 37120, this document along with ISO 37150 and ISO 37151 are implementation guidance. The difference there is this document focuses on data exchange and sharing for smart community infrastructures.

In addition, this document is also relating to standards as below:

— ISO 8000-110 Data quality - Part 110: Master data: Exchange of characteristic data: Syntax, semantic encoding, and conformance to data specification

— ISO 22745-1 Industrial automation systems and integration -- open technical dictionaries and their application to master data -- part 1: overview and fundamental principles

169 — ISO/IEC JTC1 30182

Guidelines on Data Exchange and Sharing for Smart Community Infrastructures

1 Scope

This document gives guidelines on principles and the framework for data exchange and sharing to entities having authority to develop and operate Community Infrastructure:

The guidelines of this document are applicable to communities of any size that are engaged in the data exchange and sharing of community infrastructure. However, the specific practices of data exchanging and sharing of community infrastructures depend on the characteristics of each community.

Note: The concept of smartness is addressed in terms of data exchange and sharing of community infrastructures, in accordance with sustainable development and resilience of communities as defined in ISO 37100.

2 Normative references

There is no normative reference in this document.

3 Terms and definitions

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

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

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

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

3.1 Terms relating to smart community infrastructure

3.1.1
community
group of people with an arrangement of responsibilities, activities and relationships

Note 1 to entry: In many, but not all, contexts, a community has a defined geographical boundary.

Note 2 to entry: A city is a type of community.

[SOURCE: ISO 37100:2016, 3.2.2]

3.1.2
community infrastructure
systems of facilities, equipment and services that support the operations and activities of communities

Note 1 to entry: Such community infrastructures include, but are not limited to, energy, water, transportation, waste and information and communication technologies (ICT).

[SOURCE: ISO 37100:2016, 3.6.1]

3.1.3
data ownership
the legal right of possession, including the right of disposition, and sharing in all the risks and profits commensurate with the degree of ownership interest or shareholding, as demonstrated by an examination of the substance, rather than the form, of ownership arrangements relating to smart community infrastructure data

[ADAPTED FROM SOURCE: ISO 10845-6:2011, 2.11]

3.1.4
digital continuity
an integration process to enable digital governance, digital ability, digital services and digital ecosystem construct to ensure digital data to be available, traceable and consistent with the quality characteristic of authenticity, reliability, integrity and usability along data lifecycle; a holistic approach to provide exchanged or shared data for community infrastructure

Note 1 to entry: Continuity refers to capability to manage risks and events that could have serious impact on community infrastructure to continually deliver services at agreed levels.

[ADAPTED FROM SOURCE: ISO/IEC 20000-1:2011, 3.28]

3.1.5
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1 to entry: The concept of organization includes, but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

Note 2 to entry: In this document, the concept of organization refers to an entity/institution inside the community that is tasked with implementing the management system, e.g. the local government. The community identifies an organization that it entrusts with the implementation of this document.

[SOURCE: ISO 37100:2016, 3.2.3]

3.1.6
smart community infrastructure
community infrastructure with enhanced technological performance that is designed, operated, and maintained to contribute to sustainable development and resilience of the community

[SOURCE: ISO 37100:2016, 3.6.2]

3.1.7
smart community infrastructure data
data created, captured, collected or curated from the various sources of smart community infrastructure

3.2 Terms relating to smart community infrastructure data

3.2.1
availability
property of being accessible and usable upon demand by an authorized entity

[SOURCE: ISO 27000: 2016, 2.9]

3.2.2
authenticity
property that an entity is what it claims to be

[SOURCE: ISO/IEC 27000:2016, 2.8]

3.2.3
data
reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing

Note 1 to entry: Data can be processed by humans or by automatic means.

[SOURCE: ISO/IEC 2382:2015, 2121272]

3.2.4
integrity
property of accuracy and completeness

[SOURCE: ISO/IEC 27000:2016, 2.40]

3.2.5
metadata
data about other data

[SOURCE: ISO 14721:2012, 1.7.2]

3.2.6
reference data
domain and community standardized data objects that define the set of permissible values to be used to populate other data objects

[SOURCE: ISO 5127:2017, 3.1.10.19]

3.2.7
reliability
property of consistent intended behavior and results

[SOURCE: ISO/IEC 27000:2016, 2.62]

3.2.8
shared data
data that can be accessed within an existing software application as well as between different software applications, that may be executed asynchronously or concurrently

[ADAPTED FROM SOURCE: ISO/IEC 2382:2015, 2122341]

3.2.9
thematic data
data about specific business, which is used to support decision making rather than daily operation, it can be used to supply of sustainable information resource service if required.

Note 1 to entry: Thematic data can refer to gridded data whose attribute values describe characteristics of a grid coverage feature in a grid format)

Note 2 to entry: Gridded data are data whose attribute values are associated with positions on a grid coordinate system

[SOURCE: ISO/TS 19163-1:2016, 4.14]

3.2.10
data spectrum
differentiation of data assets on the basis of whether they are considered closed,sharable or open

3.3 Terms relating to smart community infrastructure data exchange and sharing

3.3.1
data access
right, opportunity, means of finding, using or retrieving data

[ADAPTED FROM SOURCE: ISO 15489-1:2016, 3.1]

3.3.2
data acquisition
process of capturing, collecting, receiving and storing data

[ADAPTED FROM SOURCE: ISO/IEC 2382:2015, 2122168]

3.3.3
data classification
Identifier of a computer-readable representation of data for a specific application

[SOURCE: ISO 13281-2:2000, 4.2]

3.3.4
data creator
organization that creates, captures, collects or transforms data for, e.g. a city or services

3.3.5
data owner
Designated curator for the community infrastructure data related to a city service

3.3.6
data publisher
Organization that performs the publication role for community infrastructure data

3.3.7
data exchange
accessing, transferring, and archiving of data

[ADAPTED from SOURCE: ISO/TS 13399-5:2014, 3.7]

3.3.8
data sharing
a reference for providing shared, exchangeable and extensible data to enable community infrastructure

3.3.9
information security
preservation of confidentiality, integrity and availability of information

Note 1 to entry: In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

Note 2 to entry: Security refers to freedom from unacceptable risk.

[SOURCE: ISO 37100:2016, 3.4.13]

3.3.10
risk
effect of uncertainty

Note 1 to entry: An effect is a deviation from the expected — positive or negative.

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

Note 3 to entry: Risk is often characterized by reference to potential events (ISO Guide 73, 3.5.1.3) and consequences (ISO Guide 73, 3.6.1.3) or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood (ISO Guide 73, 3.6.1.1) of occurrence.

[SOURCE: ISO 37100:2016, 3.4.12]

4 Principles for data exchange and sharing

4.1 General

This document shows various possibilities to use data exchange and sharing of community infrastructures. The expectations of the outputs of this use are often very high. However, it should be noted that there are many different constraints on the range and validity of the output of data exchange and sharing. Examples are data reliability, availability, quality, complex relationships and temporal interpretation of data.

4.2 Principles

The following principles should be considered:

a) The community infrastructure data should be available to be exchanged and shared, ensuring that a balance between data security and privacy are maintained.

b) The data should have sufficient quality to enable the exchange and sharing of the community infrastructure data.

c) The data owner has the accountability and responsibility to enable the exchange and sharing of the community infrastructure data.

d) The data creator should maintain the integrity of the community infrastructure data to be exchanged or shared.

e) The data publisher should meet all the legal and regulatory requirements related to the exchange or sharing of the community infrastructure data.

f) The security of the community infrastructure data should be ensured.

g) The data should use spatial methods to achieve the positioning and control of urban infrastructure objects.

5 Type and model for data exchange and sharing

5.1 General

Smart community infrastructure includes energy, water, transport, information and communication technology (ICT), and waste. The data addressed in this document is the ones related to the infrastructures as well as built environment elements supporting the infrastructure.

With the development and complexity of the smart community infrastructure, the planning, construction, operation, management and evaluation of the smart community infrastructure information system should be based on the construction, development and utilization of the data resources, which reflect the physical/operational conditions and interactions which are defined in ISO 37155-1 of these objects.

The data exchange and sharing takes place between different application services and systems on smart community infrastructure. Various types of data exchange and sharing have different data types and functions.

The data framework for a smart city and community classifies the data assets as either metadata, reference data or thematic data. The data framework shows how current city data assets are transitioned from the existing soloed service provision to an interoperable data estate.

The collected data assets relate to the data concepts specified in ISO/IEC 30182, and utilize the classifications of open, shared and closed data within the data spectrum in use by the community.

5.2 Data type

5.2.1 Metadata

Metadata is data which defines basic information about data to be used to verify the provenance and validity of the data to be exchanged and shared. An example of metadata in a smart community data framework is the data relating to the voluntary services organizations who deliver city services on behalf of the city to citizens.

5.2.2 Reference data

Reference data is any data which defines the set of permissible values for the data which is to be exchanged or shared. For example, an atmospheric temperature reading at a certain location or a video footage for a specific street which can be used for multiple purposes.[1]

[1] PAS_183_smart cities. Guide to establishing a decision-making framework for sharing data and information services

5.2.3 Thematic data

To deliver services to citizens, thematic data in a community should initially be the datasets and legacy data that are created, processed and managed by community. An example of thematic data is bus traffic congestion along a specific street, electric power frequency fluctuation, and pressure distribution along a specific underground water pipe line. The characteristics of Smart community infrastructure, as an integration of sub systems, should be considered in the thematic data such as interaction among other infrastructures if applicable according to ISO37155-1.

Data exchange and sharing of community infrastructure, mainly conduct between metadata, reference data and thematic data. The data types for the data exchange and sharing of smart community infrastructure are described in 5.3.

5.3 Concept model for infrastructure data

Data should be available and collectable from the community infrastructures for exchanging and sharing. The collection of data is expected to be automated via technical interfaces, such as smart meters supported by APIs.

The Table 1to 3 identify the elements of the SCCM which relate specifically to community infrastructure. Community infrastructure data which is collected may relate to characteristics, consumption, movement, presence, production, status, supply and use. These descriptions are not necessarily exhaustive or mutually exclusive.

Collectable Data	*Infrastructures*	*Data Interfaces*	*Example Observation*	*Prime Concept (SCCM[2])*
Characteristics of something	Buildings	Survey	Building use	STATE
Consumption of something	Street Lighting	Smart meters	Energy used per hour (Kwh)	CASE
Movement of something	Transport Network	Vehicle GPS	Journey destinations	PLACE
Presence of something	Waste Management	Waste bin sensors	Empty / Full	STATE
Production of something	Renewable Power Plant	Smart Grid	Energy load per hour (Mwh)	CASE
Status of something	Public Realm	Environmental sensor	Outdoor temperature	STATE
Supply of something	Water Mains	Flow sensors	Leaks	CASE
Use of something	Communication Networks	System logs	Megabytes of data used	EVENT

411 Table 1 - Description of the data collected from the community infrastructure using concepts from SCCM (Smart city concept model)

412 The collected data results in information that provides insights, the types of which are also defined in the SCCM as Operational, Critical, Analytical
413 and Strategic. The insights can help identify opportunity and rationale for sharing such data among infrastructures (see Table 2).

Collectable Data	*Resulting Data (examples)*	*INSIGHTS (SCCM)*
Characteristics of something	Building Data: dimensions; occupancy; equipment; indoor temperature; indoor air quality; gas supply pressure; water flow rates; heat delivery temperature	OPERATIONAL (examines the characteristics of things)

[2] SCCM defined in ISO/IEC 30182:2017

	Demographic Data: user registration details and profile	
Consumption of something	Energy Data: domestic use of electric, thermal, gas; district consumption; tariffs and costs	CRITICAL (real-time monitoring)
Movement of something	Transport Data: modal mix; vehicle type; vehicle id; vehicle occupancy; journey start/end times and locations; traffic speed and density; pedestrian movements; energy consumption per km; emissions/pollutants per km	ANALYTICAL (the determination of patterns and correlations)
Presence of something	Image Data: congestion; integrity of the public realm, such as road maintenance; incidents; unrest and community safety	STRATEGIC (examines outcomes related to strategic objectives)
Production of something	Energy Data: local renewable production	CRITICAL
Status of Something	Environmental Data: outdoor air quality; water quality; flood levels; noise levels; temperature; weather conditions; carbon emissions; luminescence	ANALYTICAL
Supply of something	Energy Data: network power loads.	CRITICAL
Use of Something	Network Utilization:	STRATEGIC

	number of bus journeys taken	

Table 2 - Examples of the level of insights (Operational, Critical, Analytical and Strategic) from the collected community infrastructure data

The observations are also related to concepts defined in the SCCM, including active agents or items, metrics and places. The SCCM notes that by adding the concepts of time and role to the collectable data, it would be possible to further understand relationships in the sharing of data (see Table 3).

Collectable Data	*AGENT / ITEM (SCCM)*	*METRIC (SCCM)*	*PLACE (SCCM)*	*Time*	*Stakeholder Roles*[3]
Characteristics of something Consumption of something Movement of something Presence of something Production of something Status of something Supply of something Use of something	Person or Household Building or Community Government or Municipality	Cost Frequency Quantity Scale Specification State Velocity	Location points Departure points Arrival points Transit routes Neighborhoods Districts Cities	Date/time stamp	Infrastructure owners, suppliers & operators Investors Planners Citizens

Table 3 - Examples of the observations which can be used to further understand relationships of shared or exchanged

[3] Stakeholders defined in ISO/IEC 37153:2017

5.4 Data dictionary and catalogue

Data dictionary and catalogue of data exchange and sharing can be considered as an efficient approach to assist different attributes in formal, such as by industry, structure, format and classification. These are optional and not limited to the approaches listed below.

a) data dictionary is the definition and description of the data items, data structures, data streams, data storage, processing logic, and external entities that constitute the data resources of a domain.

b) data catalogue is the presentation of data resource organization and relevance, including catalogue, dictionary identification scheme and development of guidelines related to recognition system. The form is based on open technical dictionary databases as the core.

The architecture is based on the open technical dictionary (OTD) of ISO 8000 and ISO 22745 series, and its establishment and maintenance.

5.5 Data spectrum

5.5.1 General

To understand how a community can maximize the value of its data, it is important that the data framework classifies data for use and differentiates the data it holds based on whether it is considered closed, shareable or open. The extent to which the restrictions have been implemented can vary depending on the security, access and control requirements. The use of data within the data spectrum is restricted to the use, reuse and the purpose for which data can be shared. ISO 31000 outlines good practice on the management, assessment and analysis of risk and can be used by the community when implementing the data framework.

An appropriate risk management regime for the sharing, publishing and reuse of data should be established and implemented.

5.5.2 Closed data

Closed data is data which is restricted for use. This data should be designated as information that is not permitted to be shared. In a community, this data includes payment details for citizens within a specific service, such as their council tax.

5.5.3 Shared data

The shared data is the data which exist and cannot be considered as either open or closed data. This varies between cities and is assumed to represent the majority of the data in a community.

This document specifies in detail on:

— the suitability of sharing data for new purposes (see Clause 8); and

— access rights to data (see Clause 9).

It is important as part of the data spectrum to understand there are three top level access restrictions which apply to shared data:

a) specific access is when the data owner makes data accessible to either named individual(s) or named organization(s);

b) group access is when data is made available to specific groups of people or organization(s) based on predetermined criteria; and

c) public access is when data is made available publicly but only under certain terms and conditions that cannot be considered open.

Publishers of community data have a duty of care when restricted data is considered for sharing to ensure that potential harm to individuals or assets is considered prior to publication. An example of shared data such as this is COMAH (control of major accidents and hazards) data.

5.5.4 Open data

This document uses the definition of open that is maintained by the Open Project.

"Open" means anyone can freely access, use, modify and share for any purpose (subject at most to guidelines that preserve provenance and openness). This definition is also used to determine whether data can be classified as open data.

6 Opportunities for data exchange and sharing

6.1 General

The availability of open data enables smart community to explore the value of data to improve city services. However, the majority of data with a smart community is not suitable to be opened due to privacy and security considerations. With the appropriate access restrictions the three types of shared data can be unlocked for the benefit of the city and its citizens. The value of shared data includes but not limit to optimizing infrastructure services, promoting business, facilitating urban planning, enabling proactive maintenance, promoting environmental protection and improving safety and security, however they articulate a diverse range of options for all smart cities when community infrastructure data is shared.

6.2 Optimizing infrastructure services

Data exchange and sharing can provide citizen with better services including water, gas, electricity, housing, transportation, waste disposal, information services. For example, citizens get one-stop, comprehensive and efficient government information services through data exchange and sharing between government departments.

Through data exchange and sharing of community infrastructure, city managers and related providers of public services can not only optimize the construction of community infrastructure, but also can improve efficiency in daily management of community infrastructure, as well as operation and monitoring. For example, street light poles can be shared by many user. They can be used as charging points to provide energy for electric vehicle. They can be equipped with billboard. By installing various sensors or cameras on the street light poles, they can monitor traffic, noise, weather conditions. Therefore, it is very important that the information can be shared.

6.3 Promoting business

Data exchange and sharing improves the efficiency of resource allocation and promotes business development. For example, a developer can effectively utilize the shared data from community infrastructure such as telecommunication capacity, water supply capacity from infrastructure companies, number of passengers from one station to another to exploring best location for building a new hotel, to save development cost to a certain extent.

Data exchange and sharing provides opportunities for innovation and creating new business models in a community. For example, the traffic data of existing transportation and that of the movement of citizens, when combined could be used to create a field of business for driverless taxis.

6.4 Facilitating urban planning

Data exchange and sharing can help city planners draw up comprehensive infrastructure space planning, which can enhance the development and utilization level of urban space, achieve the balance between urban and rural infrastructure and make a city more harmonious and livable.

Through data exchange and sharing, control and avoidance guidelines between adjacent infrastructures can be met, planning errors can be effectively avoided, problems caused by insufficient space reservation of infrastructure can be reduced, and the efficiency of government examination and approval can be improved. For example: by data sharing, a certain distance both vertically and horizontally between power and gas supply pipelines can be maintained to ensure safety.

Data exchange and sharing can help city managers make infrastructure collaborative implementation plans. Through collaborative construction of various infrastructures, the refinement of urban planning and management can be promoted, and blind excavation, duplicate construction and resource waste can be avoided.

6.5 Enabling proactive maintenance

Data exchange and sharing can be used for more efficient and preventive maintenance of smart community infrastructures. It can provide timely relevant information to infrastructure owners, decision makers, operators or other relevant stakeholders regarding the infrastructure operation condition, first signs of defects or malfunctioning etc., enabling efficient and cost saving maintenance activity.

Additional analysis of the collected data enables predictive maintenance aiming at proper budgeting, planning and cost saving for maintenance activities. Proactive maintenance enabled by collected and shared data should additionally increase safe usage and operation of smart community infrastructures. For example, combined with the data of road traffic and people flows, street light switching times can be adjusted to save energy and improve the efficiency of operation and maintenance.

6.6 Promoting environmental protection

Data exchange and sharing can promote environmental protection. Through data exchange and sharing, community infrastructure systems can be designed to suppress the extent of pollution and more efficiently use resources such as materials and energy, including reduction of the amount of waste. It can limit impacts on existing green spaces (e.g. parks, wetlands, watercourse buffers, existing trails) and control of surface run-off and drainage.

Data exchange and sharing of community infrastructure also contribute to the improvement of public health. For example, the integration of air quality data, heating information and traffic data can help city managers adopt propriate heating and traffic control measures to avoid further deterioration of air quality.

6.7 Improving safety and security

Community infrastructure data can be utilized to improve the safety and security of services across a community. For example:

— Data integrating information of the geographical location of gas piping, communication and electrical lines help community managers with disaster management. In the event of earthquakes,

fires, floods and other natural disasters, real-time sharing of data can support government in dealing with these emergency situations more effectively.

7 Security of data exchange and sharing

7.1 General

The underlying premise of smart cities is that the greater quantity of data available from community infrastructures should be exchanged and shared to maximize the availability, reliability and resilience of city service provision for the benefit of citizens.

The use of technology is a significant enabler of improved services based on data exchange and sharing. However, this creates an increased dependence on such technologies particularly when this enables new service delivery models. It also creates significant vulnerabilities and associated security issues.

The multiple agencies and organizations participation model of smart city is made up of several agencies and organizations that can be provide different city infrastructure. In this model, all agencies and organizations which involve in providing infrastructure are responsible for maintaining the safety and security of data exchange and sharing.

The approach needed to ensure the security of data for a smart city differs from any security policies and processes which might already be in place for community infrastructure at an individual services provision level. The data security for smart city infrastructure needs to respond to the new or increased threats which exist as a result sharing and exchanging available data.

7.2 Data security approach

Security of the community infrastructure data which is exchanged and shared needs to take a holistic city-wide approach, should be appropriate and proportionate, and should aid the delivery of the city's vision and objectives. To ensure a holistic data security approach, the security measures used need to take into account physical, cyber, personnel and cyber physical aspects of community infrastructure services. This means security of data exchange and sharing should be treated as a whole; separate security planning should be avoided.

A key aspect of secure community infrastructure data provision is to consider data from city services which cross the boundaries of individual service providers (e.g. transportation, water, waste, etc.) and provide effective and secure data use for the delivery of city wide services.

A holistic data security approach with appropriate and proportionate security measures should be introduced to deter and disrupt hostile, malicious, fraudulent and criminal behaviors or activities which threaten community infrastructure.

The vulnerabilities of community infrastructure data exchange and sharing arise because:

- Differing organization priorities of individual infrastructure service providers.
- Incompatible governance arrangements, policies and processes of infrastructure providers.
- The aggregation of community infrastructure data with a wider range of data sourced for inside and outside of the city.
- Different levels of security understanding and concerns across community infrastructure providers.

- A difference in the range of risk appetites to manage data security across the city and community infrastructure providers.

The volume and accelerating pace of data generated, collected, utilized and stored adds to the security vulnerabilities of sharing and exchanging community infrastructure data. Security measures need to consider the specialist data exchange and sharing requirements (e.g., the aims and subsequently usage after the user obtains the exchanged and shared data) of personal data, intellectual property and commercially sensitive data which facilitates the provision of city wide services.

It is important to consider the threat from actors who seek to undermine any vulnerability in the data security measures for community infrastructure. These actors may be associated with organized crime seeking to acquire unauthorized personal or sensitive data, intellectual property and commercially sensitive data. It is important to consider potential acts of terrorism whose perpetrators are seeking to sabotage the exchange and/or sharing of community data to disrupt city services or compromise the city's infrastructure and the safety and security of citizens.

7.3 Security strategy and policy

7.3.1 General

For a smart city to obtain and retain the public trust, it needs to be able to respond to increasing public awareness and any potential concerns regarding the exchange and sharing of community infrastructure data. A city should be prepared to put in place appropriate mechanisms to maintain the trust of its citizens. A city needs to be capable of responding to increasing public awareness and potential concerns about how city data is being used, and put in place mechanisms to prevent the erosion of public trust.

When determining appropriate security governance for community infrastructure data, it is important that security measures consider citizens who are residents, visitors and those who enable the efficient provision of city services.

7.3.2 Security strategy

Cities should operate different service delivery options and ownership of the community infrastructure provision may be complex and will affect the data security measures which can be deployed. Cities need to consider the autonomy service providers have when devising the appropriate data security measures to be implemented.

The data security strategy which the city develops needs to consider the secure delivery of community infrastructure and all aspects of the services deployed including particularly:

- The safety of data sharing and exchange.
- The authenticity of the data exchanged and shared.
- The availability, provenance and reliability of community infrastructure data.
- Confidentiality and commercial sensitivities of service data.
- Appropriate measures to ensure the integrity of data exchanged and shared.
- Resilience requirements of data exchanged and shared.
- Interfaces are sensitive points for data exchange and sharing and data access permissions need to be put in place.

A city needs to develop a security strategy which articulates the overall security policy for community infrastructure, and how data which is to share and exchanged should be collected, managed and processed. This security strategy also needs to consider whether the security policy is justified in accordance the legislation or regulation of the appropriate jurisdiction for the city. The security policy can also be used as the basis to develop and deliver additional community infrastructure services for the benefit of citizens.

7.3.3 Security policy

The data security measures which need to be considered for community infrastructure data exchange and sharing should include the following key areas:

- Governance
- Service personnel
- Citizens
- Service delivery organizations
- Appropriate and proportional city-wide security processes
- Physical security required for the city services

It is important to ensure that the data security measures are set in the context of the complexity of the community infrastructure and the scale of the city where the infrastructure operates. The data access permissions should be limited to a small and trustworthy group of people.

7.3.4 Accountability and responsibility

The approach to data security should enable an appropriate, across the multi-agency model for the provision of community infrastructure in a city. Moreover, this security approach can also support the development of the data framework and enable the city to determine the accountability and responsibility of each community infrastructure service provider.

As the maturity of the secured data exchange and sharing of the data framework evolves, city decision makers should be appointed to reflect this changing data landscape. The changes to the data framework may arise for a number of reasons including;

- the introduction of new community infrastructure
- changes to contractual arrangements for exiting services.

The benefit of this approach to data security is that the city will curate the data which is routinely shared and exchanged, and is therefore able to understand the normal operating procedures. This can equip city leaders to ensure that city service providers are both accountable and responsible for the secure sharing, processing and exchange of community infrastructure data.

7.4 Assessment of security risks

7.4.1 Threat landscape

Smart city leaders need to understand the threat landscape which needs to be mitigated for their city. There need to be an understanding of the range of threats the city faces which should be based on vulnerabilities which might:

- Disrupt or corrupt data from community infrastructure services.
- Acquire personal data, intellectual property or commercially sensitive data related to community infrastructure services.
- Compromise the use, operation or value of city infrastructure services.
- Lead to the targeting of city wide vulnerabilities by one or more organization related to the exchange and/or sharing of community infrastructure data. For example, the targeting of integrated transport and traffic management services.
- Have the potential to be subject of sabotage via either internal or external attacks. For example, damage caused by malwares, hackers or disaffected personnel.
- Compromise cyber physical systems resulting in damage to the physical community infrastructure.
- Thefts (blackmailing, utilization, impairment, …).
- Operational risks (EDV program bugs, complexity of handling, dysfunction, …).
- Financial risks.

An assessment of the threat landscape should consider that attacks could result in loss of confidentiality, availability, safety, resilience, possession, authenticity, utility and/or integrity of data which is exchanged and shared by community infrastructure service providers

City leaders should ensure that any potential for insecure or poorly maintained services to leak, expose or permit unauthorized access to data which is exchanged and shared is considered. An attack on these infrastructure services could result in a city-wide vulnerability being created.

Contractual arrangements should be in place for the providers of city infrastructure services to enable interoperable data exchange and sharing. It is important to consider whether these contractual arrangements give additional access to other organizations' intellectual property and/or commercially sensitive data, or give extended access to another service providers' infrastructure data than would normally be the case under existing contractual arrangements.

7.4.2 Management of security risks

7.4.2.1 General

There needs to be effective management of security risks for all community infrastructure services. City leaders should ensure all relationships related to the access to data for community infrastructure service provision are specifically managed to mitigate the security risks which have been identified.

7.4.2.2 Personal Data

To provide interoperable community infrastructure services, the city should exchange and share personal data across more organizations than currently is the case. Any security breach of personal data should be avoided as this results in damaging to citizen(s), the organization, potentially damage citizen trust and therefore is damaging to the city as a whole Once there is a personal data security accident, it will endanger citizens, infrastructure agencies and organizations. It will prejudice citizen's trust in agencies and organizations. Then, it will put influence on the whole city.

7.4.2.3 Metadata

Metadata provides information about the data which the city exchanges and shares, for example the usage and access rules which apply to data in the data framework. This community infrastructure meta data represents an additional security risk. Should there be a breach of metadata this would reveal key details of how the community infrastructure data is managed. Specific security measures should be introduced to ensure the effective management of metadata.

7.4.2.4 Reference data

Reference data does not need regular updates and does not change regularly in terms of content. For example, the tolerances of sensors or the location of key buildings. However, the potential impact of an attack on this data has city wide implications and has significant impact on community infrastructure services. Specific security measures should be introduced to ensure the effective management of reference data.

7.4.2.5 Aggregated data

To provide, monitor and maintain community infrastructure services, data which is exchanged and shared should be aggregated. This aggregation may lead to increased risks and sensitivities for individuals, groups of individuals and organizations. Particular combinations or absence of data might allow directly or by inference the identification of citizens with particular health conditions. For example, specific security measures should be introduced to ensure the effective management of aggregated data.

It is important that the risks of aggregating data which is exchanged and shared also considers the security measures which are required to mitigate the threat of aggregated data being used in malicious pattern of life analysis.

8 Data privacy

8.1 General

The considerations of data privacy are of equal importance to those guidelines related to the security of data related to all smart city infrastructures in a smart city. Data privacy applies to all data which can be personal data or data which can be used to construct personal data about a citizen.

The multi-agency model of a smart city consists of many different organizations, each of which have the responsibility of delivering city services and all of whom share responsibility for the preservation of the privacy of citizen data.

The data privacy guidelines specified in this document are limited to the exchange and sharing of data which is used by smart city infrastructures.

8.2 Privacy guidelines and activities

8.2.1 General

The data privacy protection detailed in this document is to be used by smart cities to determine the privacy and confidentiality protection required for data relating to individuals and organizations involved in the provision of city services. Specifically, these privacy protection guidelines relate to those organizations participating in the data exchange and sharing of smart community infrastructures in smart cities.

8.2.2 Privacy Principles

The following eight privacy principles should be applied for the exchange and sharing of smart community infrastructure data where personal data is included or can be inferred:

- Fairly and lawfully processed within the jurisdiction to which they apply.
- Obtained only for specified purposes and not further processed in a manner incompatible with those purposes.
- Adequate, relevant and not excessive.
- Accurate and up-to-date.
- Not kept for longer than is necessary.
- Processed in line with the rights afforded to individuals under the legislation or regulation of the jurisdiction it applies, including the right of subject access.
- Kept secure.
- Not transferred to countries or regions outside the jurisdiction to which it applies without adequate protection.

If any exemptions from the eight privacy principles have been determined by the smart city, these exemptions should be documented and acknowledged for each smart community infrastructure service to which they apply.

Each organization participating in the data exchange and sharing of smart community infrastructure data should ensure that these privacy principles are carried out consistently within the requirements and guidelines of the smart community infrastructure service to which it applies.

8.2.3 Consider city stakeholders

The eight privacy principles should apply to the exchange and sharing of data for all smart community infrastructure services during design, build and implementation of each city community infrastructure service. Consideration should be given to all stakeholders for example public, patients, students, clients, suppliers, business partners and city service organizations.

At all stages of the implementation of the city community infrastructure service, the data owner, data publisher and service user roles should be identified and considered alongside the privacy preservation principles. Organizations should be identified and the data responsibilities they hold should be determined. Additionally, the appropriate mechanisms should be implemented to facilitate confidential exchange and sharing of smart community infrastructure data.

Smart cities should ensure the explicit identification and documentation of the high-risk categories of personal data processed by the city service organizations because of the operation of smart community infrastructure services.

High-risk categories of personal data can include:

- Sensitive personal data as determined by legislation or regulatory regimes.
- Personal bank account and other financial information.
- National identifiers, such as national insurance numbers.

- Personal data relating to vulnerable adults and children.
- Detailed profiles of individuals.
- Sensitive negotiations which could adversely affect individuals.

It is important that the smart city takes account of community infrastructure services where high volumes of personal data are processed and appropriately manages the increased level of risk in these circumstances.

8.2.4 Specific thematic data

Each smart community infrastructure organization participating in city data exchange and sharing should have their own guidelines to protect some data related to the service, for example intellectual property rights, commercially sensitive data, etc. These organizations should be considered when developing the appropriate data exchange and sharing mechanisms for each smart community infrastructure service. It is important to recognize where specific data can be considered that not only privacy but also security implications. Were such data to be inadvertently or deliberately made available it could have implications not just for individuals or the city service, but for the whole city.

8.2.5 Operational guidelines

Once smart community infrastructure systems are implemented, they form important and sometimes essential city services. The smart city expects to apply urban management, personalization and customization of any or all of these services. During the operation of these services, it should inevitably change the privacy mechanisms, rules and policies which govern the exchange and sharing of data. The identified roles and responsibilities should be managed in order that any changes needed are appropriately reflected. These measures should allow the update of all aspects of the management strategy such as:

- Updating of internal service rules.
- Interaction rules between organizations.
- Operational process changes.
- Protective measures such as defining new roles.
- Changes to data access management rules.
- Maintenance responsibilities.

In each of these cases where operational changes are required, a city should ensure that this also involves the examination of guidelines for authentication, authorization, access and audit.

8.3 Privacy strategy and governance

8.3.1 Senior management team

The smart city should ensure that a senior management team is tasked with issuing and maintaining a privacy policy that sets a clear framework and demonstrates support for, and commitment to the exchange and sharing of smart community infrastructure data. This should include managing compliance with data protection legislation, regulation, and application of appropriate good practice policies.

8.3.2 Privacy policy

The privacy policy should state that it covers either:

- The entire city and the organizations who deliver services.
- Identified organizations involved in the design, build, implementation or delivery of smart community infrastructure services.

The privacy policy should be communicated to all personnel responsible for delivering smart community infrastructure services in the city.

8.3.3 Accountability and responsibility

The city should designate a member of the senior management team to be accountable for the privacy guidelines of city services. The designated team member should be accountable for the management of privacy, exchange and sharing of data for the city. This team member should also be responsible for compliance with data protection legislation, regulation and endeavor to demonstrate and promote a good privacy practice regime.

The complexity of a smart city and its services may require a number of officers responsible for the establishment of appropriate data exchange and sharing policies and compliance activities. The privacy procedures should ensure that:

- The city service organizations process personal data fairly and lawfully.
- The city service organizations process personal data only where this is justified.
- The city service organizations process sensitive personal data only where this is necessary for the city service organizations purposes and is justified in accordance with the legislation or regulation of the appropriate jurisdiction.

Any individual or organization supplying personal data to the city should be provided with access to the exchange and data sharing rules which should be applied. This should require the city to produce a privacy notification which needs to clearly communicate the following information:

- The identity of the city service organization.
- The purposes for which data is to be exchanged, shared or processed.
- Information about the disclosure of exchanged or shared data to third parties.
- Information about an individual's right of access to personal data when data is exchanged, shared or processed.
- Whether personal data is transferred outside the legislative or regulated jurisdiction without adequate protection.
- Details of how to contact the city with queries related to the processing of data which is exchanged or shared.
- Details of any technologies, for example cookies, used on a website to collect personal data about individuals.
- Any other information that would make the processing fair.

8.3.4 Privacy processes

A smart city should incorporate privacy processes which ensure that any city organization shares personal data with another city organization for the provision of city services The responsibilities of both parties with regard to the data exchanged or shared are in line with smart city privacy policy. These privacy processes should be formally documented in a written data agreement or contract as appropriate.

Privacy processes should incorporate procedures which ensure that, where each organization is using the data for the provision of community infrastructure services:

- The written agreement or contract describes both the purposes for which the data may be used and any limitations or restriction on the use of the data.

- Each organization provides an undertaking or evidence of its commitment to processing the data in a manner which does not contravene the smart city privacy policy.

The privacy policy should incorporate procedures which ensure that, wherever possible, any new processing which involves the exchange or sharing of data with third parties is compatible with the privacy notification policy of the city, and the terms of privacy notifications provided to the individual,

Where this is not possible, the community infrastructure organization should ensure that it has:

- A legal basis for the data exchange and sharing.

- If required, the individual's consent to the data exchange and sharing.

Where data exchange and sharing with third parties is permitted without the consent of the individual, the privacy process should incorporate procedures, which ensure that an auditable record of the protocols and controls for this data exchange and sharing is documented.

Where data exchange and sharing with third parties are required, for example, by legislation, the privacy process should incorporate procedures, which ensure that the protocols and controls for the data exchange and sharing are documented.

8.3.5 Privacy rights of individuals

Irrespective of who was the creator of the personal data, it is important to recognize that individuals have rights their own data. The privacy process should include procedures, which ensure that individuals' rights in relation to their data are respected, and that requests to exercise such rights are dealt with within any statutory time limits. Privacy rights include access to information, objection to processing, and review of automated processing.

8.3.6 Complaints and appeals

The privacy process should incorporate a complaints procedure which ensures that complaints about the exchange, sharing or processing of personal data are handled correctly. This should include procedures for considering appeals by individuals about the way their complaints have been handled.

9 Data roles and responsibilities

9.1 General

The data related to smart cities should contain citizens' behaviour, location, trajectory, and communication records, which are regularly and automatically collected by all kinds of fixed and mobile terminals, sensors, cameras and applications.

While the value of continuously collected data increases, security threats to data are also increasing. Data roles and responsibilities should clearly include the obligation to facilitate privacy and security measures.

9.2 Data roles

Although individual cities have their own data value chain, there are five key roles to be fulfilled to maximize the impact of the data framework in a city.

The roles that exist across the data value chain include:

a) Data creator

The data creator role defines those organizations who collect and/or transform data for the city or its services. This role can be passive where the organization is responsible for the creation of data for a city, as part of the provision of a city service, for example the creation of the city data relating to the location of lampposts in the city. Additionally, this role can be a reactive role where operational insight data is collected and is transformed to provide the city with critical insight, for example a transport operator in a city who supplies data collected from cameras in the event of a critical incident. For derived or aggregated data, the data creator is the provider of the process which transforms the data created by others.

b) Data owner

The data owner is the designated curator for the data related to a city service on behalf of the city. The responsibilities of this role include the authority to change the data where appropriate and maintain the transparency for the provenance of the data within the data framework on behalf of the city.

c) Data custodian

The data custodian role differs to the data owner role as this organization does not own the data, it merely is the custodian of the data for a specific purpose or task related to the provision of a service within the city

d) Primary publisher

The primary publisher role relates to the organization that performs the publication role for all data across the data spectrum. All sources of data can be viewed by the organization who performs this publisher role, all data however might not be published. Publication of the data depends on which part of the data spectrum the data belongs to and the access restrictions which apply.

e) Secondary publisher

In a smart city an additional publication role exists. The publication of some of the data on the data spectrum is facilitated by the primary publisher. As a result, for some of the published data an organization creates additional value from the city data which has been published. This secondary organization should be encouraged to publish the new value data which has been created, performing the role of secondary publisher. The secondary publisher should monitor the quality of the data in the

data framework, feeding back to the city on any variance detected as part of the data publication process. Any access restrictions to the data to be published as part of this secondary publication role are determined by the primary publisher. A feedback loop should be incorporated which supports the primary publisher delegating authority to the secondary publisher to oversee the publication of the data itself

f) Users

There are numbers of organizations which can have differing roles in the data value chain but are also considered to be the users of city data. Although this varies between cities, the key user groups that are common to all cities are:

- City organizations which support the operation of city services, for example emergency services, community health services and contractors;
- Third sector organizations providing or supporting city services;
- Business users, for example corporations and SMEs;
- Citizens;
- Academic organizations:
- Other cities;

9.3 Provenance of data

The metadata and reference data within the data framework should be specific to a city and is crucial to understand the provenance of data to have effective data exchange and sharing of city infrastructure data. The value of the city data can be unlocked by ensuring that the smart city infrastructure data is findable, accessible and interoperable as below.

- Findable

mechanisms which ensure the data is discoverable and identifiable.

- Accessible

licenses and/or license restrictions that are applicable to the use of the data and how the data is made accessible for use by third parties.

- Interoperable

the extent to which the data are made available to all organizations for use or reuse.

The data framework provides a useful tool acting as an inventory of the smart city infrastructure data, facilitating city leaders to identify the potential impacts and benefits of sharing and exchanging smart city infrastructure data.

9.4 Accountability

Data owners are accountable for ensuring that data collection, exchange and sharing processes are implemented in a consistent manner across all city infrastructures, particularly in terms of the underlying definition of metadata and reference data, data quality, protocols and formats.

City stakeholders encounter number of general problems that are the result of inherited siloed data estates, for example:

- Fragmented datasets
- Different temporal framework
- Different spatial footprint
- Different granularity
- Differing and proprietorial formats
- Different definitions of same datasets
- Low motivation to share

Consequently, issues of ownership and associated intellectual property rights can act as barriers to the exchange and sharing of city infrastructure data and create obstacles to the realization of the value in the data framework.

Nonetheless it is in the wider interests of city data owners to accommodate the sharing and exchange of data between city infrastructure services to promote investment in city infrastructure that maximizes city performance, reduces costs, harmonises the needs of citizens, supports city leadership, the environment and promotes sustainable development and city resilience.

9.5 New business models

There are many new business and commercial models which could support the creation of the data framework and overcome the siloed data legacy.

One example of this is a city data cooperative, as an accountable trusted partner. This business model is a mechanism to provide the collaborative framework to develop and support a range of quality and accountability agreements for smart city infrastructure data. A city data cooperative could be formed to reduce the burden of exchanging and sharing of data between infrastructures. These organizations create quality protocols providing and useable data formats to maximizing the benefits of exchanging and sharing of smart city infrastructure data.

As infrastructure owners, suppliers and operators make use of big data generated by city activities and interactions, cities should continue to develop use cases, around which standards are agreed, leading to practical templates and processes that support good data governance.

9.6 Standards Framework for Cooperative models

A standards framework for cooperative data exchange and sharing should include the Interfaces, Processing, Integration, Measures and the assessment of Impacts on a scale for each city area and organization affected using the Smart City Concept Model defined in ISO/IEC 30182. Technical standards for other interfaces, such as devices and meters, are already well established.

Integration standards include the technical aggregation and management of data with the assignment of interdependent roles among data controllers, processors, integrators and suppliers which support the legislative and regulatory jurisdiction for the city.

Regarding the measurement of impact smart city indicators, such as those recommended in ISO 37120:2014, help interpret impacts for the four levels of insight, operational, analytical, strategic and critical as defined in ISO/IEC 30182:2017 Smart City Concept Model.

To understand impact, standards which prepare impact assessments should closely align with ISO 37153:2017.

This is a complex and well served standards arena. PAS 183:2017 gives appropriate guidance to be used for the exchange and sharing of smart city infrastructure data.

10 Use cases

Project title	Beijing Almighty Virtual Card application and security management Platform – A Case study for Security of Community Infrastructure Data Exchange and Sharing
Project profile	Security guidelines: In Beijing, mobile virtual cards are needed to implement different government departments issue and management, as well as citizens daily activities concerning acquisition of food, clothing, shelter, transportation, entertainment, education, medical care, and payment for water, electricity and gas. It is required to ensure security for citizen identity information in the process of providing access to these activities with convenient and low cost. The Beijing virtual card security management platform is based on virtual cardholders, the application of terminal unique identification authentication, encryption and virtual CARDS in the process of transaction security barrier protection. It will greatly reduce the risk of existing information and data security threats by the use of a decentralized offline authentication mode, the online maintenance, security management of virtual CARDS and virtual POS greatly by reducing the overall operating cost and social cost. By these means, the Beijing Almighty Virtual Card application and security management Platform provide a big data source for community analysis and decision making, the mutual trust and security guarantee mechanism of community infrastructure data exchange and sharing is formed. The Beijing Almighty Virtual Card Management Platform includes three parts: 1) basic guarantee system; 2) the Beijing Almighty Virtual Card System and 3) a data operation platform. On security design, the project follows the principle of protecting the weakest link, integrity, consistency, least privilege, operability, combining technology with management and other principle of security designs. Transaction security technology includes anonymous technology, identity authentication technology, anti-duplication trading technology and anti-counterfeiting technology. In terms of network system security, the project divides the network domain into parts with different security levels, between which firewall and access control policies limit illegal access. The network audit system and intrusion detection system are used to increase the detection and audit of network

		security incidents. Through the credible guarantee technology by provision of an ECC chip, secure container and the life cycle management, a safe and trusted application environment are provided for the distribution, circulation and transaction of virtual cards. To ensure that the application system's database systems are secure, such as transaction and communication security, user access control, and data security, powerful encryption techniques - an asymmetric key system, Combined Credit Key System (CCKS) is used in this project, which enables identification without the need for the support of a third-party certification center (CA)which can support offline authentication in IoT and real time anti-counterfeiting, deploys rapidly and lower cost. In addition, the pre-access service system is used to access the virtual card SDK, which provides access to account management and transaction services for virtual CARDS. The exchange system can be deployed with multi-node and handle the requested routing processing, transaction processing, transaction process management, etc.
Organization		Organizer: Beijing Municipal Commission of Economy and Information Technology Main participants: Beijing Municipal of Health and Family Planning; Beijing Municipal Civil Affairs Bureau; China Smart City Technology Co., Ltd; Cyber Nerv Communications Inc.
Place		Beijing
Time		2016-2017
Reference		1. Construction Plan of Beijing Almighty Virtual Card Platform V1.0 2. Smart community Public Information Platform Construction Guide (Trial Version). 3. URL: http://www.beijing.gov.cn/bmfw/cxfw/bjt/
Relevance to this document	7.2,4	Security principle, governance and strategy
	9.2,3	Privacy guidelines, strategy and governance
	10	Data ownership and responsibility

993

Annex A (informative)

Case study

A.1 Data exchange and sharing for community infrastructure based on "Map World · Nanjing"

Project title	Data exchange and sharing for community infrastructure based on "Map World · Nanjing"
Project profile	With the continuous development of Smart Community, the demand by government departments for spatial and other information applications are also increasing. The need for data sharing is very strong. Based on "Map World · Nanjing", the Nanjing government builds up community infrastructure public service platform and establishes an integrated map of all kinds of community infrastructure data. The platform provides portal, standard online service, API, front server, mobile APP, and other application patterns. It carries out community infrastructure data sharing and exchange. It also plays an important role in smart community, mainly including portal, data management system, service publication system, catalogue and data exchange system, operation management system and collaborative management system. This case study constructs a smart community infrastructure data system, and could provide services for data integration, synthesis and management. A framework for data exchange and sharing is established. Based on data security within the life cycle, smart community infrastructure data exchange and sharing could be completed. Regarding the data type, the platform constructs community infrastructure data systems for "energy, water, transport, waste, ICT", and feature refined. Besides the property of geo-information, smart community infrastructure also contains abundant thematic information and reference information. The data management system can realize the effective organization and management of multi-type and multi-format data. The data fusion, catalogue and data exchange system is based on the CSW directory service specification, and provides service registration, discovery and binding to achieve interoperability between national, provincial and municipal community infrastructure service. Based on "Map world · Nanjing", the platform could carry out data integration, synthesis and management in the fields of rail traffic, sewage, rainfall, etc. and establishes one map of community infrastructure data. Regarding the data sharing and exchange framework, the service publishing system provides online information services and supports service-based application construction with regular programming languages. The platform provides a variety of shared patterns such as portal, standard service, API

		development, server front, mobile APP, etc. Regarding the data security, the operation management system realizes platform users and authority management, service management and service application operation status monitoring.
Organization		Project owner : Nanjing Urban Planning Bureau Main participants: Nanjing Urban Planning Research Center, Wuda Geoinformatics Co., Ltd, JianYe District People's Government, Gaochun District People's Government, Qixia District People's Government, YuHua District People's Government, Jiangning District People's Government, Nanjing municipal Public Security Bureau, Nanjing Urban Management Bureau, Nanjing Bureau of Land and Resources, Nanjing Municipal Environmental Protection Bureau.
Place		Nanjing China
Time		2016-2017
Reference		1. Technical Requirements of Provincial and Municipal Level Nodes of Map World. 2. Guidelines on construction of Smart City Public Information Platform.
Relevance to this document	6.4	Facilitating urban planning
	6.5	Enabling proactive maintenance
	10	Data ownership and responsibility

A.2 Data exchange and sharing for community infrastructure based on the "Beijing Almighty Virtual Card"

Project title	Beijing Almighty Virtual Card application and security management Platform – A Case study for Security of Community Infrastructure Data Exchange and Sharing
Project profile	Security guidelines: In Beijing, mobile virtual cards are needed to implement different government departments issue and management, as well as citizens daily activities in food, clothing, shelter, transportation, entertainment, education, medical care, and pay for water and electricity gas. It requires to ensure security for citizen identity information in the process of trading these activities with convenient and low cost. Beijing virtual card security management platform is based on virtual cardholders, the application of terminal unique identification authentication, encryption and virtual CARDS in the process of transaction security barrier protection. It should greatly reduce the risk of existing information and data security threat by using of decentralized offline authentication mode, the online maintenance, security management of virtual CARDS and

	virtual POS greatly by reducing the overall operation cost and social cost. By these ways, Beijing Almighty Virtual Card application and security management Platform provide a big data source for community analysis and decision making, the mutual trust and security guarantee mechanism of community infrastructure data exchange and sharing is formed. Beijing Almighty Virtual Card Management Platform includes three parts: 1) basic guarantee system; 2) Beijing Almighty Virtual Card System and 3) data operation platform. On security design, the project follows the principle of protecting the weakest link, integrity, consistency, least privilege, operability, combining technology with management and other principle of security designs. Transaction security technology includes anonymous technology, identity authentication technology, anti-duplication trading technology and anti-counterfeiting technology. In terms of network system security, the project divides the network domain with different security levels, between which firewall and access control policies limit illegal access. The network audit system and intrusion detection system are used to increase the detection and audit of network security incidents. Through the credible guarantee technology by providing ECC chip, secure container and the life cycle management, it provides a safe and trusted application environment for the distribution, circulation and transaction of virtual cards. To ensure that the application system's database systems are secure, such as transaction and communication security, user access control, and data security, powerful encryption technique - an asymmetric key system, Combined Credit Key System (CCKS) is used in this project, which enables identification not needing third-party certification center (CA) supporting, can support offline authentication in IoT and real time anti-counterfeiting, deploys rapidly and lower cost. In addition, the pre-access service system is used to access the virtual card SDK, which provides access to account management and transaction services for virtual CARDS. The exchange system can be deployed with multi-node and handle the requested routing processing, transaction processing, transaction process management, etc.
Organization	Organizer: Beijing Municipal Commission of Economy and Information Technology Main participants: Beijing Municipal of Health and Family Planning; Beijing Municipal Civil Affairs Bureau; China Smart

		City Technology Co., Ltd; Cyber Nerv Communications Inc.
Place		Beijing
Time		2016-2017
Reference		1. Construction Plan of Beijing Almighty Virtual Card Platform V1.0 2. Smart community Public Information Platform Construction Guide (Trial Version). 3. URL: http://www.beijing.gov.cn/bmfw/cxfw/bjt/
Relevance to this document	7.2,4	Security principle, governance and strategy
	9.2,3	Privacy guidelines, strategy and governance
	10	Data ownership and responsibility

1001

Bibliography

1) ISO/IEC27000 2014Information technology — Security techniques — Information security management systems — Overview and vocabulary.

2) ISO/IEC 27001:2013(EN) Information technology — Security techniques — Information security management systems — Requirements

3) ISO/IEC 27002 2005 Information technology — Security techniques — Code of practice for information security management.

4) ISO/IEC 27003 2010 Information technology — Security techniques — Information security management system implementation guidance

5) ISO/IEC 27004 2009 Information technology -- Security techniques -- Information security management – Measurement

6) ISO/IEC 27005 2011 Information Technology – Security techniques - Information security risk management

7) ISO/TS 37151 27005 2011 Smart community infrastructures —Principles and requirements for performance metrics

8) Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

9) ISO/IEC 11770-1:2010 Preview Information technology -- Security techniques -- Key management -- Part 1: Framework

10) ISO/IEC 11770-3:2015 Preview Information technology -- Security techniques -- Key management -- Part 3: Mechanisms using asymmetric techniques

11) ISO/IEC 15946-1:2016 Preview Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 1: General

12) Xianghao Nan， Combined Public Key (V8.0)， International Journal of Automation and Power Engineering (IJAPE), 2014，3：119-123

13) ISO/IEC TR 29181-5:2014 Information technology -- Future Network -- Problem statement and requirements -- Part 5: Security

14) A Soft Key System and Its Implementation (China Patent: 201510028842.2).

15) A New Terminal Security Soft Key Management Method (China Patent: 201510690811.3)

16) GB/T 25056-2010 Information security techniques - Specifications of cryptograph and related security technology for certificate authentication system

17) GB/T 20988—2007 Information security technology -Disaster recovery specifications for information systems

18) GB/T 33132-2016 Information security technology—Guide of implementation for information security risk treatment

19) ISO/IEC 27033-1:2015 Preview Information technology -- Security techniques -- Network security -- Part 1: Overview and concepts

20) PAS 183:2017 Smart cities – Guide to establishing a decision-making framework for sharing data and information services

21) BSI: 2015. City data survey report for BSI in support of understanding data requirements and standards for smart city initiatives.

22) https://www.bsigroup.com/Documents/BSI_City%20Data%20Report_Singles%20FINAL.pdf.

23) BSI: 2016.European Innovation Partnership for Smart Cities & Communities (EIP-SCC). EIP-SCC Urban Platform Management Framework. Enabling cities to maximize value from city data. Ver 03 October 2016. https://www.bsigroup.com/Sustainability/EIP_Mgnt_Framework.pdf.

24) BSI: 2017. European Innovation Partnership for Smart Cities & Communities (EIP-SCC). Rethinking the city: using the power of data to address urban challenges and societal change A guide for city leaders.https://www.bsigroup.com/Sustainability/EIP_Leadership_Guide.pdf

25) BS ISO/IEC 30182:2017. Smart city concept model. Guidance for establishing a model for data interoperability.

26) BSI.PAS 183:2017 Smart cities – Guide to establishing a decision-making framework for sharing data and information services

27) ISO/DIS 37120 :2017 Sustainable development in communities -- Indicators for city services and quality of life (taking place of ISO 37120:2014 Sustainable development of communities -- Indicators for city services and quality of life

28) ISO/DIS 37155:2017 Smart Community Infrastructure Maturity Model

29) Imperial College, London (2016) D8.1: Common monitoring and evaluation framework (CMEF), Sharing Cities project funded by EU Horizon 2020

30) BSI (2017), Smart City Concept Model ISO/IEC 30182:2017

31) Teeside University (2016), D1.3 Data Management Plan, Demand Response in Blocks of Buildings (DR-BOB) project funded by EU Horizon 2020

32) TNO (2016) D2.1: Definition of data sets, CITYkeys project funded by EU Horizon 2020

33) ISO 13281-2:2000, Industrial automation systems and integration—Manufacturing Automation Programming Environment (MAPLE) — Part 2: Services and interfaces

34) ISO/Guide 73:2009, Risk management — Vocabulary

35) ISO/IEC/IEEE 24765:2010, Systems and software engineering — Vocabulary

36) ISO 10845-5:2011 ,Construction procurement — Part 5: Participation of targeted enterprises in contracts

37) ISO/IEC 20000-1:2011, Information technology -- Service management -- Part 1: Service management system requirements

38) ISO 14721:2012, Space data and information transfer systems — Open archival information system (OAIS) — Reference model

39) ISO/TS 13399-5:2014, Cutting tool data representation and exchange -- Part 5: Reference dictionary for assembly items

40) ISO 9000:2015, Quality management systems — Fundamentals and vocabulary

41) ISO/IEC 2382:2015, Information technology -- Vocabulary

42) ISO 15489-1:2016, Information and documentation — Records management — Part 1: Concepts and principles

43) ISO 37100: 2016, Sustainable cities and communities — Vocabulary

44) ISO/TS 19163-1:2016, Geographic information — Content components and encoding rules for imagery and gridded data — Part 1: Content model

45) ISO/IEC 25066:2016, Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- Common Industry Format (CIF) for Usability -- Evaluation Report

46) ISO 5127:2017 , Information and documentation — Foundation and vocabulary

