ITU-D Study Groups

**Study period 2018-2021**

**Question 1/2**

*Creating smart cities and society: Employing information and communication technologies for sustainable social and economic development*

**Annual deliverable 2019-2020**

# Promoting trust and safety for the creation of smart cities and communities

## Executive summary

In smart cities and communities, the data generated, collected and used by connected objects are myriad and diverse. Massive data collection brings with it potential vulnerability to attacks targeting connected devices. Proportionate, risk-based solutions can help prevent attacks and provide protection, addressing issues such as infrastructure vulnerability, trust in connected objects and protection of personal and proprietary data.

This annual deliverable touches on these different risks and perceived threats, while fundamentally addressing ways to improve and/or manage the security of architecture, infrastructure, networks, and data generated or collected from smart city and community applications. This deliverable highlights case studies detailed in contributions received.

## Contents

## 1. Introduction

Smart cities and communities offer numerous opportunities to improve lives in multiple facets of the urban and rural ecosystems, which can include public safety, transport, environmental management, economic development, and support for innovation, tourism, health, education, civic engagement, e-government, and workforce development among other opportunities.

Smart city and community projects are likely to be more successful where applications are relevant to community needs and trusted, therefore accepted and well-used.

Moreover, as stated previously, the success of smart city initiatives depends to a large extent on user trust in the digital infrastructures and services on offer.

For the construction of new smart cities and communities, as well as the addition of new smart applications to existing communities, designers should follow an approach inspired by sustainable development based on traditional community development planning in line with an assessment of user/stakeholder needs. Similarly, the proportionate and legal use of massive data generated by the city's activities can enable better planning. As smart city and community development and implementation occurs, we observe that data derived from new applications are driving decision-making across disciplines at the city, state/provincial and regional level.

Policy-makers must also address in their planning the need to securely generate, transmit and store the massive amounts of data that will be a defining feature of smart cities and communities.

### 1.1. Building trust first

Successful smart cities and communities and the applications they use must rely on the implicit trust of consumers if they wish to see mass adoption. The concept of smart cities and communities encompasses the notion of safe and trusted cities. Cybersecurity, when factored into the design of smart-city projects and applications, is key to promoting and maintaining trust.

*Cybersecurity, when factored into the design of smart-city projects and applications, is key to promoting and maintaining trust.*

Trust is one of the most important considerations for residents of cities and communities, and the need for trust and public safety is well understood.

The contributions received reflect this: the concept of trust in smart cities and societies includes cybersecurity, cyberhealth, disaster management and public safety. These categories do not stand alone but are interconnected. Consequently, all measures and systems should be considered. For example, a big challenge for policy-makers is how to manage networked government services efficiently and sustainably, while protecting personally identifiable information. An example that one country has pursued involves the use of sensors to locate citizens during their evacuation to community shelters following a disaster, to register the number of people in each shelter and inform relatives of their safety.

There are several factors behind the importance of trusted smart-city infrastructure for the development of the IoT and smart cities.

One potential risk for trust in smart cities is a city's adoption of hardware and software before all critical systems have been tested. City/community leaders should pursue risk-mitigation strategies when planning for the introduction of new hardware and software systems, including accountability measures for both procurement officials and vendors.

Security considerations and measures should be part of the whole lifecycle and core considerations in the architecture, design and deployment

Policy-makers and other decision-makers should also consider the use of open-source software, which allows for independent testing and public review for vulnerabilities and effectiveness.

Some smart city systems use encryption-free wireless communications, which may increase the risk of data theft, interruption, or other cyberattacks, including denial-of-service attacks on cities' servers. For example, some view wireless devices with limited resources, if not properly configured and deployed as susceptible to data interception and spoofing (e.g., imitating the IP address of a device on a given network in order to benefit from accessible services).

Sensors or other networked devices can be subject to data manipulation or exfiltration by malicious cyber actors. A network's or device's security can be compromised or disabled after the interception of a weakly secured exchange.

Malicious cyberactivity can impact critical infrastructure, which could, for example, lead to disrupted services in critical sectors, including power outages, malfunctions in hydroelectric dams and the hacking of water-treatment facilities. There are direct risks to the security confidentiality, availability and integrity of the system, with the potential for the subsequent manipulation of sensitive data. These different issues are dealt with in this document, which will address the architecture of infrastructure, connected objects and data generated or collected from people, while promoting trust among residents in a secure smart city. This document will also highlight case studies detailed in contributions received.

## 2. Infrastructure risk management

### 2.1. Stakeholders

Securing infrastructure when creating smart cities is a task that depends on the participation of all stakeholders. These typically include:

- network providers;
- device providers;
- platform, software and/or application providers;
- community leaders (both elected and appointed);
- citizens, universities, schools, hospitals, museums, light and heavy industry, etc.

### 2.2. Risk categories

Infrastructure risk management seeks to address several risk categories, including at least three broad scenarios:

- Denial-of-service attacks on critical facilities: This occurs when a perpetrator seeks to render a network resource unavailable to users by temporarily or indefinitely disrupting services of a host, often by overwhelming the host's ability to respond to requests. Denial of service can represent a significant threat in a universally connected world.
- Remote takeover of public or private facilities, in which unauthorized users gain access over connected systems: This is a major risk associated with the sharp rise in the number of connected objects. If risk mitigation is ineffective, it is relatively easy for a malicious actor to penetrate a connected device, then a network, etc. and laterally move through infrastructure. With networked objects being by definition

interconnected, if even one is vulnerable, then all objects on the same network may become vulnerable.

– Theft of proprietary or personal data: Consumers are increasingly concerned about the protection of their personal data and do not wish to expose their data to risk. In a connected world built on a foundation of data, the security of the systems that process data from consumers, residents and applications is paramount to building and maintaining trust.

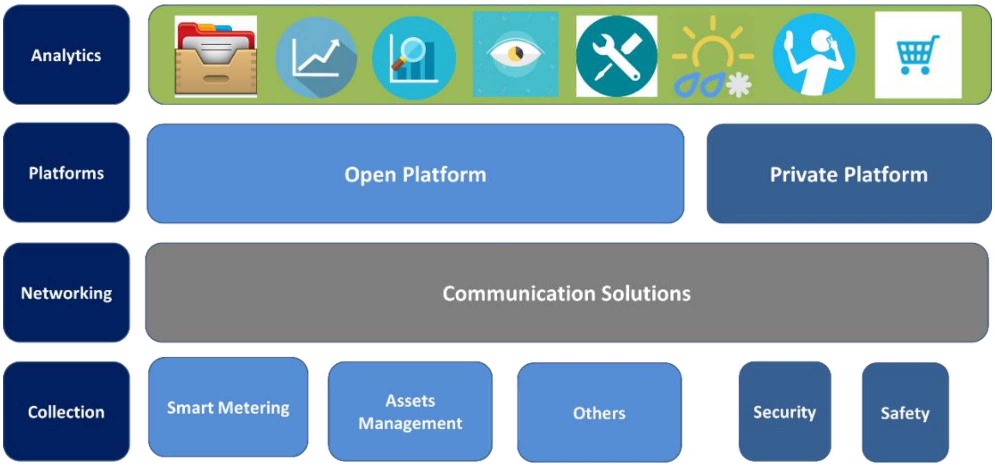
### 2.3. Safety and trust-based architecture

Policies aiming to provide the success of smart cities should address the cities' infrastructure. When creating smart cities, one of the issues to address is the availability, confidentiality and integrity of data.

*Policies aiming to provide the success of smart cities should address the cities' infrastructure. When creating smart cities, one of the issues to address is the availability, confidentiality and integrity of data.*

As shown in Figure 1 below, secure and trusted infrastructure should be considered and incorporated at each level in a smart city's architecture.

**Figure 1: Layered architecture of a smart city**



This figure describes in detail the architecture and principal components of a smart city. It conveys a layered architecture for the flow of information and collection and analysis of data.

As it demonstrates, access networks have two types of subnetwork: safety subnetwork (carrying safety-related information), which in this case is completely autonomous and cannot be accessed from the Internet; and the smart subnetwork (carrying the smart information), which can connect to the Internet.

In addition, it would be appropriate to establish a trust-based strategy and mechanisms capable of detecting and mitigating vulnerabilities at the different hardware and software layers. The strategy should include the ability to determine appropriate controls and measures to mitigate these vulnerabilities. In addition, there should be a complementary strategy to detect compromise, alert relevant stakeholders, and inform management and resolution strategies.

A secure-by-design approach should be taken when developing and deploying IoT services and infrastructure that runs through the full development lifecycle, encompassing design, development and deployment. This includes designing appropriate security and trust domains across the architecture to minimize the likelihood and effects of threats.

## 3. Confidentiality of personal and proprietary data

People are increasingly concerned about the protection of their personal data. Some of these concerns relate to digital identification, data protection and the protection of personal data.

### 3.1. Digital identification

While recognizing the importance of digital identification to the creation of ICT applications for smart society, the issue of trust and the lack of generic directives for implementing digital identification remain some of the greatest concerns regarding the introduction of such platforms. The national framework for digital identification should provide sufficient assurances on user privacy in order to engender greater trust among users and stakeholders.

> *The national framework for digital identification should provide sufficient assurances on user privacy in order to engender greater trust among users and stakeholders.*

The introduction of robust and inclusive identification systems can contribute to the efficient, precise and secured use of data. Robust identification systems have the capacity to establish not only the existence of persons within a specific jurisdiction, but also their uniqueness. There are at least three different models that can be adopted to manage a framework for digital identification, namely:

– The government is directly involved as the identity service provider.

– The government is not the identity service provider; it acts only as the regulator and provides resources such as best practices and guidelines for the private sector and other stakeholders.

– The government acts as the regulator and identity broker/clearing house, while the private sector or other stakeholders act as identity service providers.

The issue of digital identification has become more important to some countries. The World Bank estimates[1] that 1.1 billion people around the world are unable to prove their identity and find themselves deprived of social and economic benefits.

For those countries that seek digital identification, they see it as a catalyst for to help enable many smart city and community services. It can allow governments, for example, to more efficiently deliver the benefits of social programmes, such as health care, schooling, welfare, financial services, etc., and to reach the population groups in need and to target its activities based on this identification.

### 3.2. Examples of digital identification discussed in Study Question 1/2

For those countries that seek digital identification, they see it as a catalyst to help enable many smart city and community services. It can allow governments, for example, to more efficiently deliver the benefits of social programmes, such as health care, schooling, welfare, financial services, etc., and to reach the population groups in need and to target its activities based on this identification.

[1] Press release of the World Bank dated 25 September 2018.

Examples of digital identification can be found in the following countries:

**India: Aadhaar** and **DigiLocker** are biometric systems in which a random 12-digit number is assigned as a unique identity to each Indian citizen. DigiLocker is a key initiative under Digital India, which is the Indian Government's flagship programme to transform India into a digital society and a knowledge-based economy. DigiLocker is aligned with the visions of Digital India, offering citizens a private shareable space on a public cloud and ensuring the cloud-based availability of all documents/certificates.[2]

**Estonia**: The **e-Estonia** platform operates using a chip-based identification system. The government provides a PIN code to each national, based on physical identifiers, which provides access to a wide range of government services.[3]

**United Kingdom: Gov.UK Verify** allows individuals to choose a government-approved identity provider, which provides a single connection and, thereby, access to government services.[4]

**Denmark: NemID** in Denmark is a digital identification platform which provides access to public- and private-sector services.[5]

### 3.3. Regulatory and policy approaches

Interest in the issue of data protection has increased in recent years, particularly in the light of the European General Data Protection Regulation (GDPR). In Europe, the rise of the digital economy and changes in uses have compelled the European Commission to revise its rule book on the protection of personal data. Many other governments around the world are taking a variety of approaches to addressing these issues, such as drafting new data-protection laws, revising existing laws to accommodate the growing digital economy.

Information specific to persons in a smart city relates to civil status, such as surname, first name, sex, date and place of birth, address, etc., as well as social, economic and physical data, such as image, voice, fingerprint or genetic data. Some person-specific data may be processed based on obtaining the consent of the individual, or based on the legitimate interest of the person collecting the data, or to fulfil a contract, for example. More sensitive data, such as biometric data for identification and genetic data, are often subject to special requirements. For example, the collection and processing of sensitive data may be prohibited, or only permitted with consent or to protect the data subject's life (in circumstances where they are unable to provide consent). Sensitive data generally refers to data liable to reveal, directly or indirectly, racial or ethnic origins, political, philosophical or religious convictions, trade-union affiliations or information on health or sex life.

### 3.4. Directives and standards for digital identification approaches

As noted above, different governments and organizations vary in their support for national-level digital identification, and some have developed standards that could be of great use in the design and implementation of a national framework for digital identification and data security. Some of the most relevant examples are listed below:

– ISO/IEC standard 29115: "Information technology — Security techniques — Entity authentication assurance framework", a working framework for managing entity authentication assurance in a given context[6]

[2] Contribution 2/95 (BDT Focal Point Focal for Question 1/2)
[3] Ibid.
[4] Ibid.
[5] Ibid.
[6] ISO. ISO/IEC standard 29115 (2013)

- ISO/IEC standard 24760-1: "Information technology – Security techniques – A framework for identity management"[7]
- Recommendation ITU-T X.1253, on proposed security guidelines for identity management systems.[8]

Guidelines are being developed in multiple countries, such as Canada (IAM), the United Kingdom (IDAP) and the United States (NSTIC), to address possible identification, authentication and security concerns. As part of its collaboration with the United Nations, the World Bank group has produced a number of useful publications, including principles on identification. Such publications for the implementation of digital identification may help countries that choose digital IDs to plug certain gaps in infrastructure and fulfil requirements in terms of ICTs, technical standards, regulations for the development of digital identification and issues of security and trust.

## 4. Trust in IoT peripherals

Smart cities can be used to leverage digital integration to offer more efficient and effective services.[9] Inevitably, not everything is straightforward in smart cities. Some people may be wary of using and sharing their personal data, which complicates efforts to bring new technologies online at the city level.

Many smart cities are leveraging an increasing number of IoT devices, which can enable connectivity, communication and other smart-city applications. While the IoT and faster data processing continue to drive smart-city development, they also increase the need to promote trust and risk management. The very fact of connecting simple everyday objects, such as televisions, light bulbs and so forth, to a network represented a major technological breakthrough. With these new connected objects generating such positive results, issues of identity and access management were often neglected in the past. Now that IoT switches are gaining in maturity and stability, the vulnerabilities and potential risks of data loss are better understood and the management of such risks for collected data is a higher priority.

*While the IoT and faster data processing continue to drive smart-city development, they also increase the need to promote trust and risk management.*

### 4.1. Potential measures to consider

To promote trust and therefore further consumer adoption, various measures are being introduced into IoT applications, products and services. The following actions are worthy of consideration:

- Promote validated identities for smart-city infrastructure, such as having a validated identity for each connected device within the smart-city infrastructure, whether it be a streetlamp, an earthquake detector or a car, and having them properly connected to the network, with authorization for the connection and for participation in the service.

[7] ISO. ISO/IEC standard 24760-1 (2019)

[8] Recommendation ITU-T X.1253

[9] Chris Teale. Report: Smart city technology could dramatically improve quality-of-life indicators. June, 2018. According to this study, cities could reduce daily commutes by 15-30 minutes and crime by 30-40 per cent, improve emergency service response times by 30-35 per cent and even save 25-80 litres of water per person per day.

- Adopt a protection-by-design approach for data.[10]
- Have unique login credentials that require users to change them on first use in order to avoid brute force attacks, which rely on weak passwords and default login details.
- Protect network access with strong authentication measures, which could include incorporating biometric authentication in IoT devices, which would help to better reassure users.[11]
- Use strong data encryption; this measure concerns both storage and network for devices which are capable of this work.[12]
- Regularly release updates, and consider doing so via a secure channel: this helps to maintain the device through its life and keep it up to date as regards security.
- Dedicate resources to ensuring cybersecurity of critical systems and overseeing the smart-city network as a whole.

## 5. Case studies and practices

In order to resolve some issues associated with smart cities, cities and companies around the world are establishing what is sometimes called a city brain: a control centre to manage smart-city data generation, transmission and storage. Such centres may also present cybersecurity risk and should be protected accordingly.

*Cities and companies around the world are establishing what is sometimes called a city brain: a control centre to manage smart-city data generation, transmission and storage. Such centres may also present cybersecurity risk and should be protected accordingly.*

In China, city brains have been created in Hangzhou, Macao and other cities. A city brain is a platform-type AI centre built on the innovative use of big data, cloud computing, AI and other cutting-edge technologies in accordance with the urban science theory of urban life and the concept of Internet plus modern governance.[13]

In Egypt[14], the smart city architecture involves two city brains or main centres: (i) a command and control centre (CCC) that manages and handles all critical and sensitive data and (ii) a city operation centre (COC) that handles and manages operational data and services.

The city of Shiojiri in Japan provides an example of how software-defined networks and data-utilization software can resolve some smart-city issues and challenges facing residents and communities. It also demonstrates how the city's programme uses its data to provide information to facilitate services, such as for natural disaster management, crime prevention, tourism, agricultural support, etc.[15]

In Spain, Barcelona has established an urban operations and management centre to integrate all collected urban data, covering eight sectors: transport, property, security, business services, education, healthcare, sports and leisure, and government.

[10] This approach both shows that the protection of privacy and non-disclosure of personal data are priorities and allows for the protection of privacy to be incorporated in processes, procedures and activities of organizations from the outset rather than in retrospect.

[11] ITU-D SG2 Document SG2RGQ/73 from NEC Corporation (Japan)

[12] ITU-D SG2 Document 2/198 from China

[13] Ibid.

[14] ITU-D SG2 Document SG2RGQ/70 from Egypt

[15] ITU-D SG2 Document 2/208 from NEC Corporation (Japan)

In the United States, New York City uses its intelligence operations centre to support data-driven decision-making by integrating different data from various departments, including geographical information, GPS, 3D construction, statistics, cameras, etc., which enhances communication between each sector thanks to different data fusions in a unified data platform. The data are anonymized to protect residents' personal data.

In the Republic of Korea, Busan is one of the leading cities in the integration of ICTs in urban services and operations. The Busan pilot city project seeks to serve as a model of tomorrow and to create economic opportunities for economies that have adopted the technologies of the fourth industrial revolution.[16]

## 6. Findings

Based on the provided case studies, we can make the following findings and observations with regard to building trust and assuring public safety in smart cities:

- Cities need to be securer and safer as part of being smart;
- Privacy and security by design approach should be adopted;
- Safety needs also be through prediction of and following the occurrence of a disaster. ICT-based solutions and use of sensors could help predict disasters and can help locate people following a disaster;
- When fostering or creating smart cities, the availability, confidentiality and integrity of data are important factors;
- Trust should be built across all layers starting from the underlying infrastructure ending up with applications;
- For newly-built cities, one approach might be to have a separate subnetwork for safety and emergency response with redundant means of communications to be fully operational and available;
- Digital identification can help enable many online and smart services, and it needs to be well protected and secured whether provided through private sector capabilities, or as a government function;
- For some governments, successful implementation of digital identification platforms/projects depends on regulatory frameworks;
- Different jurisdictions should continue to develop their own approach to issues of personal data protection;
- Standards need to be adopted when considering identity management, authentication assurance, etc.;
- Countries need to develop their own regulations and directives related to data privacy and handling;
- Trust should be assured across IoT devices and networks to avoid data loss or data mishandling;
- Some governments seek to ensure that each connected device within the smart city infrastructure, has a validated identity and is properly connected to the network;
- Release regular updates for IoT devices as appropriate via a secured channel;
- Governments should consider dedicating resources to ensure strong cybersecurity measures are in place for all networks and devices in critical sectors;
- Where appropriate, policymakers and other decision-makers should consider using open-source software, which can be independently tested and publicly reviewed;
- Some smart cities and communities distinguish between the "command and control centre" and "city operation centre". In these instances, the command and control

[16] ITU-D SG2 Document 2/219 from the Republic of Korea

centre is in charge of assuring safety in the city and responding to all crises and emergencies while a city operation centre is in charge of provisioning smart services and applications.

---

Follow the work of **ITU-D Study Group 2 Question 1/2** *Creating smart cities and society: Employing information and communication technologies for sustainable social and economic development*

**Website**: Q1/2 website

**Mailing list**: d18sg2q1@lists.itu.int (Subscribe here)

**More information on ITU-D study groups:**
Email: devSG@itu.int Tel: +41 22 730 5999
Web: www.itu.int/en/ITU-D/study-groups

---