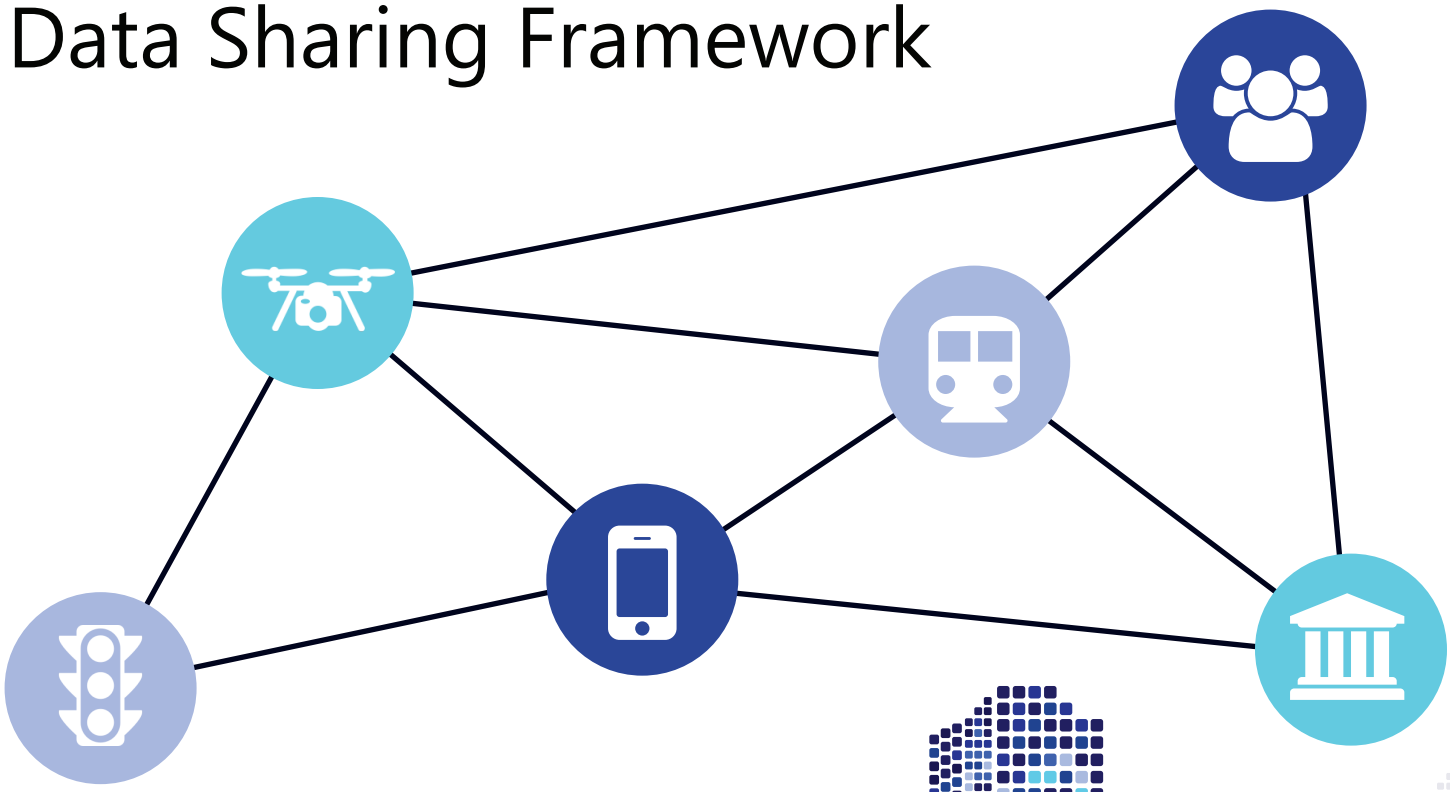
March 2018

Smart Cities

Data Sharing Framework



Abstract

As Smart City projects continue to expand and evolve, data sharing sits at the intersection of business opportunities and technology developments. Cities can certainly benefit from data sharing across Smart City applications and sectors, but sharing among cities, as well as the development of data exchanges and marketplaces, will signal that Smart Cities are moving to the next level of value creation for citizens and local governments.

This report assesses data sharing alternatives for Smart Cities and proposes a blueprint for a common framework, a set of critical components and an evolutionary path from data collection to data monetization.

Foreword

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's business priorities. ATIS' 150 member companies are currently working to address 5G, cybersecurity, robocall mitigation, IoT, artificial intelligence-enabled networks, the all-IP transition, network functions virtualization, smart cities, emergency services, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle – from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), and a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

Notice of Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to www.atis.org/01_legal/patent-policy/ to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

Copyright Information

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

Contents

1. Introduction

As a growing number of cities begin to create new Smart Cities applications — and in some cases, leverage existing investments — data will play a key role in realizing success. While Smart Cities infrastructure will serve as the engine, data sharing platforms will act as the fuel for building new applications across city resources and citizen needs.

The *ATIS Data Sharing Framework for Smart Cities* Report builds upon the recently published *ATIS Technology Roadmap,* providing an in-depth assessment of data sharing approaches, standards, applications, and monetization opportunities. The *ATIS Technology Roadmap* had previously identified advanced analytics, data integration, and data exchanges as key platform enablers. As described in that report, platform enablers support the distribution, management, exchange, and integration of data and services within a Smart Cities ecosystem.

Data sharing platforms are at an early but critical stage for many emerging Smart Cities. Data collection from IoT sensors and connected devices is creating a valuable city asset and serving as a catalyst for data to be integrated across many city resources. At the same time, applications that could leverage this data with citizens, adjoining industries and specialized agencies, are being constrained by the significant business, technology, and policy challenges associated with the sharing of data. Similarly, many cities are beginning to look at opportunities to share data on a city-to-city, regional, and national basis, with a different set of challenges and opportunities.

This report takes a holistic view of data sharing across the many facets of a city's operations and examines the different ways in which data resources can be leveraged. Creating better operating efficiencies and achieving citizen value are important catalysts for promoting investments in data sharing platforms, but new business opportunities and data monetization are key to achieving sustainability and expansion of applications and services into the future. Eventually, it is expected that data marketplaces can act as the citizen- and business-facing dimensions of a Smart City, encouraging application developers to apply data resources to the ever-expanding set of new applications they will create.

The subsequent sections of this document will provide a generic view of data sharing, which can be customized and applied to each city's unique needs. It will begin with the role of data sharing in the future and provide an assessment of the business challenges

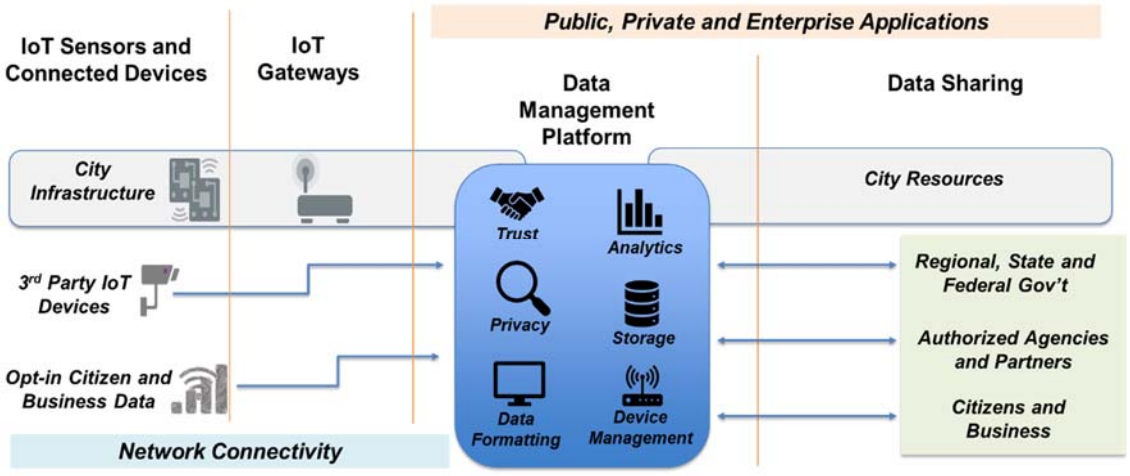
and opportunities associated with the exchange of data. A review of current approaches and trials across North America and global cities will provide a baseline of knowledge in this area. A proposed data sharing framework, and an analysis of the critical components that define this framework will help cities further visualize future opportunities. Replication and interworking can be advanced through better knowledge standards and collaborative activities that are already underway across the industry. The evolution from data exchanges to data marketplaces will help to define a future business model that applies this framework to an application-centric Smart Cities ecosystem. This report concludes with key findings and next steps in advancing this vision.

2. The Future Role of Data Sharing in Smart Cities

Data sharing represents both a requirement and an opportunity for Smart City deployments. It is clear that data sharing across citywide departments and platforms is an essential element of any Smart Cities plan. Further, cities recognize that data sharing among city resources and citizens contributes to the perception of a Smart City, functioning as a value-based ecosystem. From a policy and legal perspective, many cities are already developing capabilities that are compliant with open data obligations — either at a local or state level. All of these factors support the need for Smart Cities to invest in robust data-sharing solutions.

The concept of cities utilizing data sharing as an opportunity, both from a citizen value and a future revenue point of view, has not been fully explored across industry. Although the business aspects of Smart City data sharing will be explored in the next section, it is helpful to view Smart City ecosystems from an end-to-end perspective, looking at both sources of data and consumers of data.

The diagram below provides a functional illustration of a smart city data sharing ecosystem, and addresses both city-owned data sources, as well as devices that may operate in the citizen, business, or third-party domains. It is generally assumed that data sources that operate outside of the public sector will be accessed as part of an opt-in arrangement.



End-to-end Functional View of Smart Cities Data Sharing Platforms

Given the growth in data collected from various sources, it is generally assumed that cities will make early decisions to deploy an integrated data management platform, which is comprised of varying levels of hardware/software that supports functions like trust, privacy, storage, etc., and applies value-added capabilities, which include data analytics, device management, and data formatting. Over time, the data management platforms can incorporate new capabilities, such as predictive analytics, machine learning, and artificial intelligence.

Above the data management platform resides a robust set of applications (developed in the public or private sectors) that create value on top of collected data. While these applications may be initially focused on municipal handling of data, integrating across city resources, it is expected that consumer and business applications will leverage this abundance of data in the future and create applications that enhance perceived value and lay the groundwork for establishing revenue opportunities in the future.

It is understood that the role of data sharing will evolve as Smart Cities evolve, with cities progressing from data sharing solutions focused on public sector needs (built on a set of unique requirements) to a broader view of exchanging data across city boundaries and ultimately as part of a robust data marketplace.

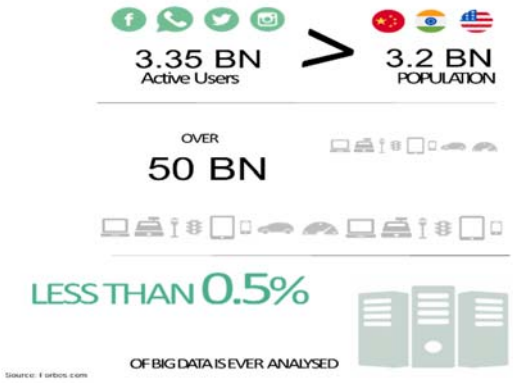
While the scope of this report is intended to address the entire data sharing ecosystem, its focus is future data sharing in the following areas:

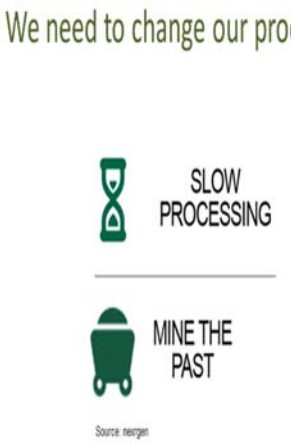
1. Among cities and other government entities (e.g., other cities, surrounding counties, state and federal government).
2. Strategic exchange of data with authorized agencies and partners (security agencies, emergency response entities, etc.).
3. Data sharing with commercial sector, private industry, citizens, and applications developers.

The intersection between city collection and management of data with these three areas has the potential to dramatically increase the value proposition associated with Smart Cities investments.

3. Business Drivers and Opportunities

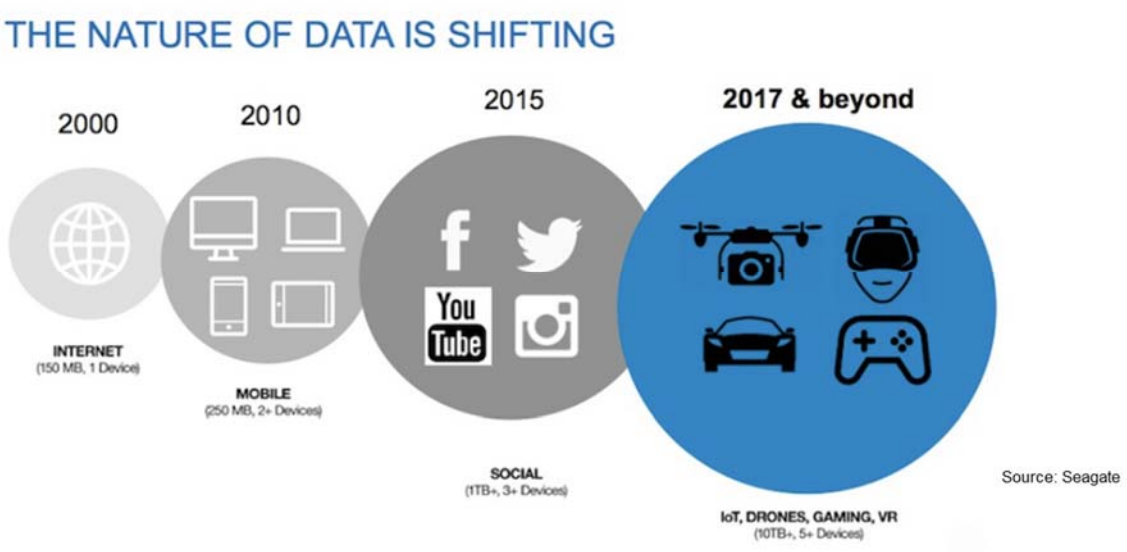
As cities continue to develop their Smart Cities plans and vision, it would be impossible to ignore the rapid pace of data growth and content sources that are impacting almost every facet of the human experience. It is widely acknowledged that more data has been created in the past two years than in the entire previous history of the human race.





At the same time, it is understood that treating this data using the same processes that have been leveraged in the past is not sustainable or beneficial. Instead, it will become increasingly important to process data at the edge (where possible), analyze data in real-time and to rapidly identify data that is relevant to the creation of value.

Network planners and application developers already embrace these changes as the market evolves from an approach of presenting data in "highly structured formats" to one of data as "unstructured content." While the nature of data has been evolving for many years, the more immediate impact of this market shift will resonate across the entire content ecosystem, including the platforms that collect, integrate, and analyze data.



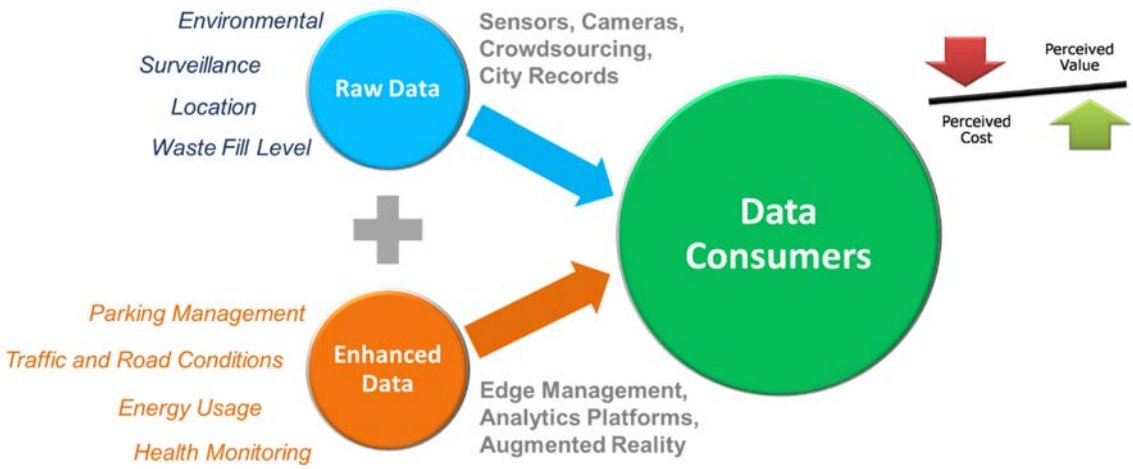
A sampling of current and future content sources presents a broad range of formats and applications that will impact Smart Cities:

- Flat text files
- Log files
- Documents (.xls, .pdf, .ppt, etc.)
- Hierarchical files (JSON, XML, YAML, etc.)
- Blogs
- Video
- Music
- Social Media Content
- Currency
- Real-time stream
- Objects
- Blocks of raw data

As data formats continue to change, solutions must reach beyond expansive centralized databases toward more robust infrastructure capable of addressing real-time data needs and new capabilities, such as predictive analytics, machine learning, and AI. The requirements surrounding real-time data will extend far beyond the concepts of sharing historical data that is static in nature.

Applying the evolving nature of data to Smart Cities will become one of the key market-changing events of the next few years. Media companies, advertisers, retail industries, and enterprises have long understood the need to monetize data and create applications, on top of data, that deliver value to their customers. Cities have a unique opportunity to leverage some key aspects of data monetization and to build these capabilities into their long-term plans and vision. The journey to monetization may be part of an evolutionary path and may involve several transitional steps, but the business opportunity is within the reach of Smart Cities if data sharing platforms are implemented in a manner that promotes exchange of data between cities and citizens, and between cities and regions.

The basic value chain for Smart Cities data is built upon a collection of raw data coupled with some level of enhanced data. In many cases, raw data will be sufficient to meet the requirements of the application. In other cases, raw data combined with enhanced data will be needed to support applications that require special formatting or application of analytics. From a value proposition perspective, the perceived value of the data (from citizens and city operations) must outweigh the cost of acquisition and management of the data — or the perceived cost.



Value Proposition for Smart City Data

4. Current Industry Approaches and Trials

Many Smart City initiatives begin with the deployment of connectivity resources (e.g., community fiber, municipal Wi-Fi) or single-purpose applications (e.g., smart street lighting, smart parking or waste management). A few cities and public-sector agencies have begun to value a more forward-looking approach that cuts across multiple Smart City applications, focusing on data as the common element. This section describes three separate projects from different parts of the world.

Data-oriented Smart City Projects

The purpose of these data-exchange profiles is to illustrate the approaches that leading-edge proponents are deploying and their emphasis on the importance of combining siloed data for ease of sharing and application innovation.

- Copenhagen's City Data Exchange (CDE) aims to break down application silos by integrating and sharing city data through a collaborative effort involving 50 companies. The scale economies resulting from this strategy lower the costs of data management for all participants. The CDE roadmap shows how cities need to think beyond the provision of raw data to future requirements in the form of analytical tools.

- oneTRANSPORT™ is a regional and multi-city initiative involving local government agencies in four UK counties: Buckinghamshire, Hertfordshire, Oxfordshire, and Northamptonshire. These local government authorities collaborated in a pre-commercialization, data marketplace trial. In this example, public and private sector data suppliers make data from Smart City and transportation assets available to data consumers (analytics specialists, application developers, etc.). The end users then leverage the data to better manage local government operations and to launch smart-city applications.

- Columbus, Ohio was awarded a $40 million Smart City grant by the U.S. Department of Transportation to test new mobility technologies with the aim of sharing lessons learned with other cities. One of the 15 projects within the Smart Columbus initiative is to create an Integrated Data Exchange (IDE) that would manage data resources from multiple sources and provide a common interface for application developers and data researchers.

Copenhagen – City Data Exchange

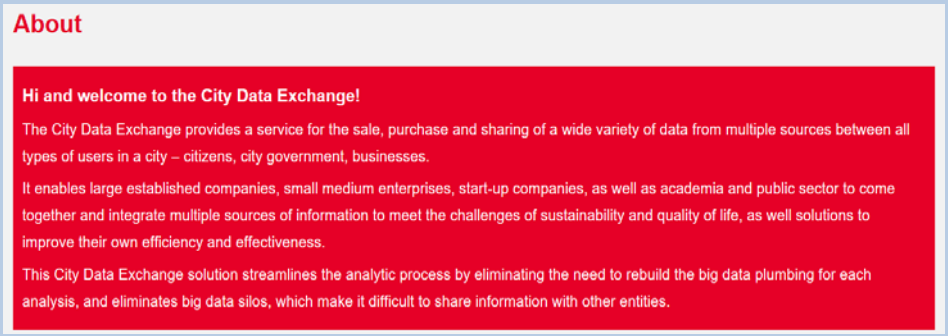
Overview & Smart City Challenge

The concept of a central data mart was conceived by Copenhagen to help achieve its goal of becoming carbon neutral by 2025.

In the past, Copenhagen has launched Smart City programs in areas such as smart lighting, traffic management, and intelligent building management. The data from these projects exist in silos. In order to build a Smart City, however, where health services, public safety, energy and businesses work together, Copenhagen recognized the need to integrate and share city data.

Implementation Roadmap

Copenhagen's City Data Exchange (CDE) marketplace for data was launched with a publicly accessible portal in May 2016. Its development involved close collaboration with more than 50 companies, which co-created the CDE with the help of several universities, non-profit organizations and other cities.



The CDE team has already discovered 65 sources of open data about Copenhagen, ranging from demographics to weather to crime statistics. The intention is to extend data coverage to categories such as city life, infrastructure, climate and environment, businesses and economy, demographics, housing and buildings, and utilities usage. The implementation roadmap begins with making raw data available to CDE users and then progressing to the addition of analytical tools.

Economics of a Shared Platform

The cost of gathering and processing the data will be recovered through subscription and service fees. These are expected to be much lower than the cost any company or city would face in performing the work of extracting, collecting, cleansing, and integrating the data by themselves.

https://community.hds.com/community/innovation-center/hus-place/blog/2016/05/31/copenhagen-city-data-exchange-can-offer-improved-services-and-create-jobs

https://www.citydataexchange.com/#/dataset/about

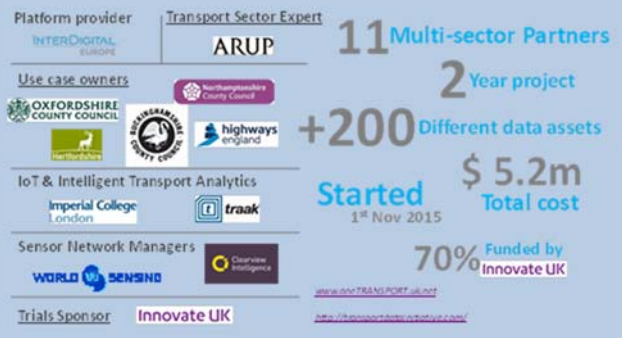
oneTRANSPORT - Intelligent Transport & Smart City Solution

Overview and Smart City Challenge

City and regional authorities operate across multiple verticals and with multiple private-sector service partners. Their responsibilities extend to communal services for residents and businesses in areas such as education, public safety, sanitation, transportation and social welfare.

The challenge for city authorities is to satisfy demand cost effectively and efficiently, recognizing the need for interoperability between the different applications and datasets managed by public- and private-sector organizations.

The oneTRANSPORT initiative in the UK is an example of such a system. The public/private partnership among 11 organizations is creating an open marketplace for data and data services.



It also obsoletes fragmentation across IT systems, transportation modes and geographic regions. Datasets belong to multiple stakeholder organizations and sources covering: traffic lights; road sensors; car parks; and static/manual generators linked to road works and cycle paths.

Standards-based Data Marketplace Solution

The oneTRANSPORT initiative used the oneM2M™ global Internet of Things (IoT) standard to overcome the technical complexities of multiple sources and siloed data systems.

By making data available in consistent formats via a unified interface, the technical solution enables basic connectivity between applications and devices, as well as interworking among devices that do not adhere to the oneM2M standard. This innovation allows data providers (e.g., owners of sensors, connected assets, public- and private-sector data streams) to interact with data consumers and enable a wide range of Smart City service providers and their applications.

Adoption Results

In the United Kingdom, the County Councils of Buckinghamshire, Oxfordshire, Hertfordshire and Northamptonshire became the first to deploy the Smart City data exchange and marketplace. Now, they can share, access and amalgamate hundreds of different datasets, enhancing the possibility of commercializing these datasets and allowing application developers to access data in a simplified manner. This environment is leveraged in Smart City and intelligent transport applications relating to ring-road congestion management, a park-and-ride scheme, and travel management for a large-scale sporting arena.

Following the first deployment, the city of Birmingham's — through its SmartRouting project — joined the platform to create a new and more accurate travelling information mobile app.

Smart Columbus

Overview and Smart City Challenge

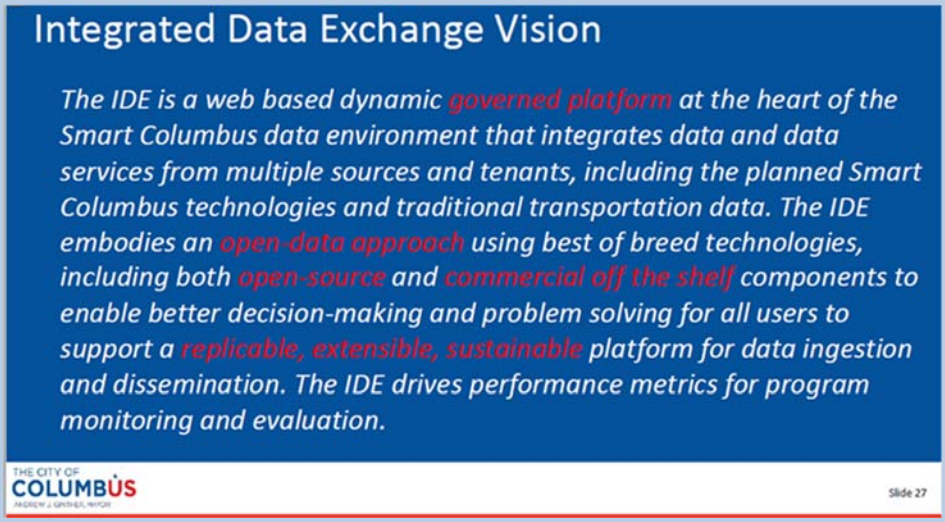
In 2016, Columbus was awarded a $40 million federal transportation grant in the Smart City Challenge. With the Smart City grant, the U.S. Department of Transportation tasked Columbus with testing new mobility technologies, promoting the goal of sharing what would be learned with other cities. Smart Columbus is pursuing this objective via 15 projects, including one focused on an Integrated Data Exchange (IDE).

Two issues drive the requirement for an IDE. One is the need for a system to manage data resources from multiple sources. The second is the need for a common interface for application developers and researchers using the data.

Vision for Smart Columbus IDE

The Smart Columbus IDE will be launched in mid-to-late 2018 and aims to:

- collect data from multiple IoT sources;
- govern access;
- ensure privacy;
- enable analysis via data APIs.



The city views the act of moving data as a new city service. Smart Columbus aims to make 50 data sets available from public sources and local and national companies. The city also is looking for additional data, "all types of it, you name it and we want it here," it says on the sandbox website.

https://www.bizjournals.com/columbus/news/2017/05/08/smart-columbus-sandbox-giving-developers-access-to.html

Smart Columbus keynote presentation by S Elhami and C Stewart (2017) – http://midas.umich.edu/wp-content/uploads/sites/3/2017/05/ChristopherStewart-Shoreh-Elhami-Keynote-reduced.pdf

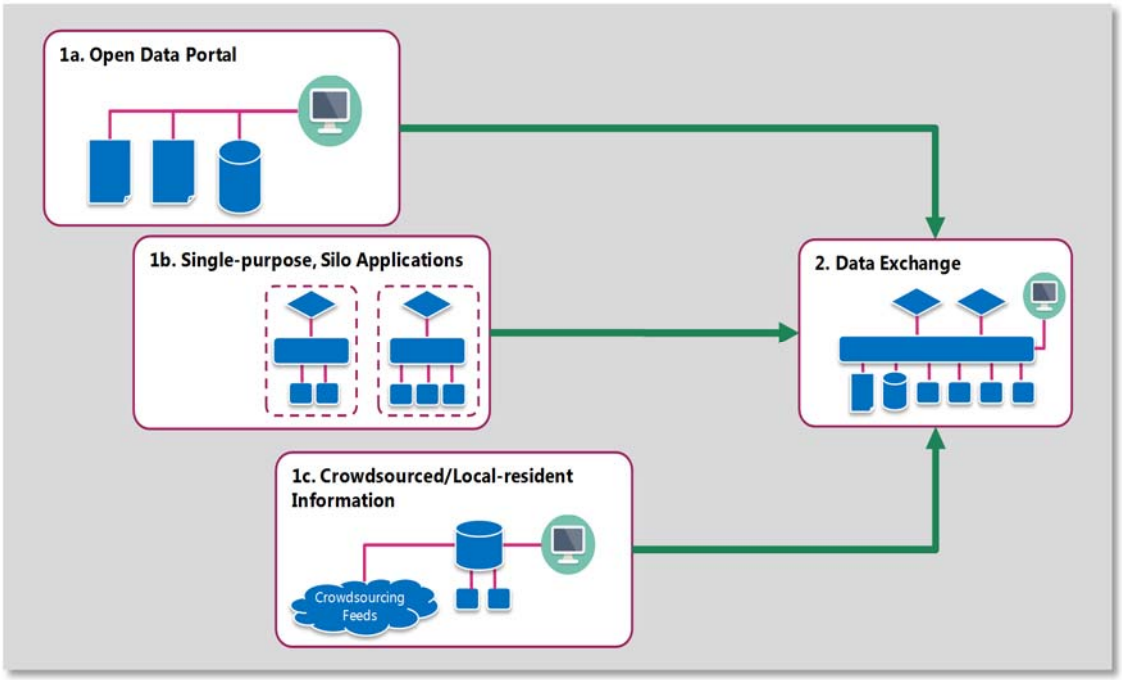
5. Data Sharing Framework

Current Smart City initiatives represent the first step of a journey that begins with a few point solutions and progressively evolves to an integrated and systematic delivery of multiple Smart City services. A data sharing framework is an important milestone in this journey, best viewed in the context of multiple data collection sources and the data management platforms that integrate, analyze, and create value for city operations, citizens, and businesses.

Most cities will implement data sharing as part of an evolutionary journey from data integration to data exchanges, and then to data marketplaces.

The following diagram illustrates the first important transition that cities will make. It joins individual, Smart City data initiatives into a systematic and scalable environment that can support numerous applications and citizen services. Cities may have one or more starting points in the form of:

- An open data portal that provides open access to city data such as road maintenance schedules, historical crime statistics, etc.
- Single purpose silo-applications, which involve data generated from city assets as that used in operational applications such as waste collection (connected garbage bins), dynamic street lighting (connected lamp posts), etc.
- Crowd-sourced, local resident information, which includes data gathered from residents via social media feeds or survey techniques (e.g., in-person, on-line applications).



Systematic approach to bring together Smart City data from multiple service initiatives

Each data gathering approach has its merits in terms of the value-add in comparison to historical city operations. Operational limitations are also a reason to implement better techniques and evolve to the data exchange model, as explained below.

Box 1a – Open Data Portal

Open Data Portal	
Solution Characteristics	• City data provided for free, with no access controls. • Static records (historical snapshot) using multiple presentation formats (e.g., city-specified format, flat file, proprietary third-party).
Incremental Value-add	• Improves government transparency, accountability, and public participation. • Can enable inter-departmental collaboration.
Limitations	• Cities forego commercial upside from downstream use of their data. • Cities incur costs to originate and publish their data.

Box 1b – Single-purpose, Silo Applications

Profile – Single-purpose, Silo Applications	
Solution Characteristics	• Applications deployed for internal operations (e.g., street lighting, traffic control, waste management). • Time-series data (enables trend and correlation analysis).
Incremental Value-add	• Improves resource use via operational efficiencies (asset/workforce management) and cost savings (e.g., smart street lighting).
Limitations	• Single-purpose application may not extend to other use cases. • Cities may incur costs to make data more widely available when relying on third-party application service providers.

Box 1c – Crowdsourced/Citizen Information

Profile – Crowdsourced/Citizen Information	
Solution Characteristics	• Citizen-sourced data obtained directly (e.g., dedicated, city applications) or indirectly (by parsing social media feeds). • Time-series data (enables trend and correlation analysis).
Incremental Value-add	• Ensures government responsiveness via direct public interactions.
Limitations	• Applicability limited to specific use cases. • Social media feeds are not representative (e.g., skewed to younger residents, out-of-towners).

Box 2 – Data Exchange

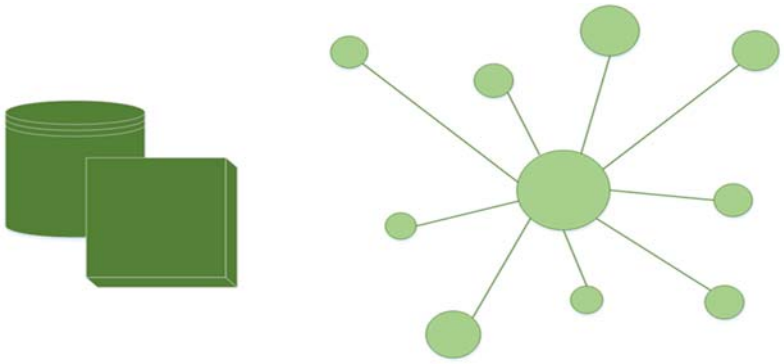
Profile - Open Data Portal	
Solution Characteristics	• Common environment to bring together multiple sources of data (static and time-series) in a standardized format. • Can integrate third-party data (e.g., weather, traffic).
Incremental Value-add	• Enables economies of scale (shared technology and support staff resources). • Encourages collaboration and the use of uniform implementation approaches across the organization (i.e., breaks through operational and technical silos). • Formalizes quality-of-service characteristics, providing greater design reliability for application developers.

Profile - Open Data Portal	
Limitations	• Data limited to internal use (i.e., "walled garden"). • Data exchange solves a technical challenge but not the wider application and data-monetization commercial opportunities.

Data Exchange Network Models

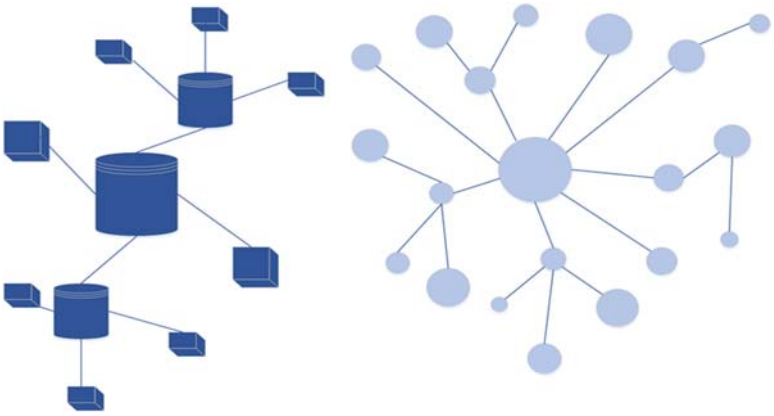
At a high level, data exchange architectures incorporate on the following approaches: centralized, distributed and decentralized. In some cases, one approach may act as part of a transition from one architecture to a more complex solution. In the case of Smart Cities, it is expected that centralized models may expand to distributed or decentralized arrangements, as cities begin to exchange data with other cities, or Smart Cities evolve to smart regions. Geographic differences, resiliency needs, and public/private data-sharing among cities will likely guide city adoption of the appropriate approach. Below is a simple representation of each architecture:

- Centralized (One Data Exchange holds all data)



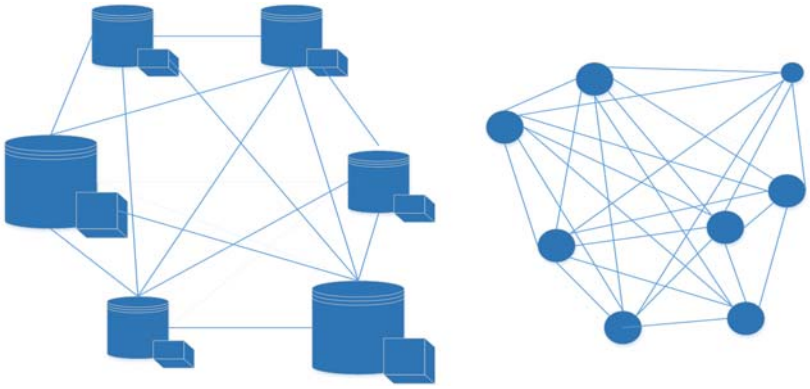
In a centralized network model, collected data is primarily processed, analyzed, stored and shared in a core data center location or group of locations. This is a generalized big data approach and provides economies of scale for treatment of large-scale data.

- Distributed (Data Exchange accesses Data on the sub-nodes)



In a distributed data model, a core data center is connected to a number of distributed sub-nodes to minimize the cost of transporting all data to a centrailized location and to allow a higher degree of data management near the edge of the network. This approach may be efficient in a Smart Region to maximize sharing of geographically relevant data for macro-applications.

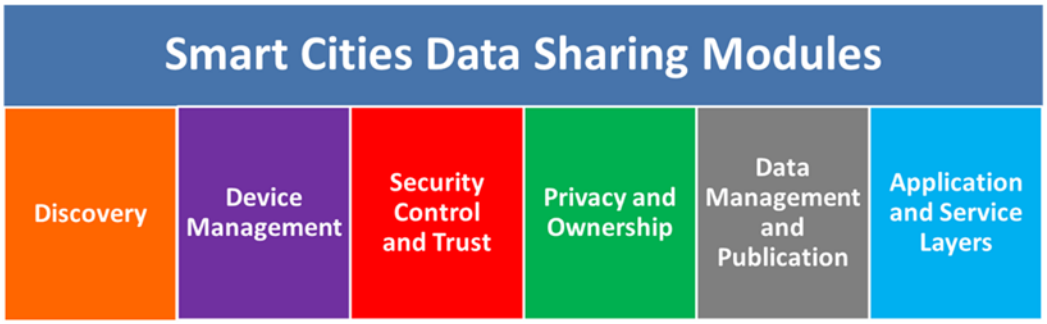
- Decentralized (Peer-to-Peer Content Exchange)



Decentralized network models repesent a future architectural choice for cities to share data with other cities, state, or federal agencies in a peer-to-peer content exchange arrangement. While the data within a city may be centralized, the data exchange among cities or within a federation is viewed in a decentralized manner. It is possible that a decentralized model that is shared among geographically dispersed entities could be overlaid on top of a centralized or distributed model within a city or region.

6. Critical Components of Smart Cities Data Frameworks

This section will provide a modular "plug-in" view that is consistent with industry approaches but can be understood through the prism of Smart Cities needs and language.

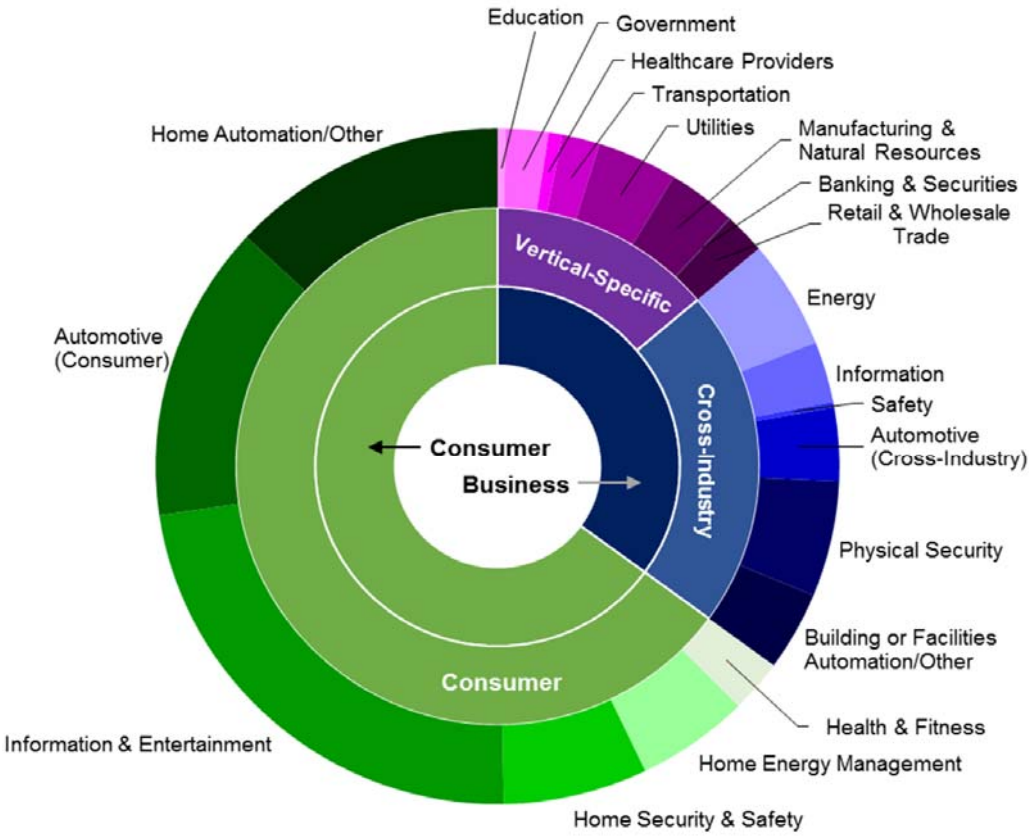


Discovery

The discovery framework for IoT-based devices, both within a set of city resources and with third-party or consumer/business-owned devices, will play a major role in the success and scale of Smart City applications.

In order to highlight the significant impact of discovery in a Smart City fabric, it is important to acknowledge the universe of potential IoT-connected devices. Gartner estimates "that by 2020, there will be 9.7 billion connected things in Smart Cities, and 81% of those things will come from smart home and smart commercial building sensors." The projected allocation of IoT endpoints across market sectors is illustrated below:

IoT Endpoints Forecast for 2020 (by Sector)



Source - Measuring the Strategic Value of the Internet of Things for Industries – Gartner, April 2016

This forecast highlights the abundance of consumer-owned devices, but it also shows the significant contribution of vertical-specific and cross-industry devices that can deliver valuable data to the Smart City ecosystem.

Sensors, actuators, and other control-based devices have existed for many years as part of municipal and utility infrastructure and have generally been managed as part of closed-system architectures. The emergence of IoT devices coupled with Smart City applications has set the stage for an exponential growth of connectivity that will leverage public and/or commercial networks in the future. The ability to discover these devices in an effective manner will depend heavily on a consistent, standards-based approach. This includes both devices and services discovery, which will in turn promote discovery of applications and resources that can create value for Smart City participants.

There exist many device and service discovery protocols in use today (e.g., mDNS, DNS-SD, Physical Web). Nevertheless, given the scale of IoT devices and related applications in the future, discovery should be considered as part of the larger ecosystem of IoT common functions to promote interoperability. Two of the most significant efforts underway, focused on developing a holistic and interoperable framework for IoT devices, are oneM2M and the Open Connectivity Foundation (OCF). For additional details on these projects, see Annex A.

Device Management

At a fundamental level, device management is focused on maintaining the reliable connectivity of a device and monitoring the configuration and secure operation of the device. There are several important elements of device management that should be applied to Smart Cities infrastructure and connecting devices:

- *Secure Configuration Management and Control* — Authenticated registration, service provisioning and connectivity management
- *Monitoring and Remote Diagnostics* — Remotely monitoring performance parameters (e.g., battery life) and event-driven messages, and applying this information to preventative and remote diagnostic actions
- *Software Management* — Maintaining consistent software configurations within server/client environment and applying feature updates and security vulnerability fixes from a centralized environment

Using unmanaged IoT devices can be a nightmare for any Smart City deployment. Concerns range from stolen devices (allowing criminals access to the data within) to devices that consume excess resources (thus damaging the experience of other users on the network, recruited into a botnet, or even become a launching point for a malware attack against other local devices).

Device management gives cities the ability to fight back against these concerns, even when the IoT device is permanently installed in a hard-to-reach location. Device management addresses the full range of possibilities that a connected device invites over the years of Smart City deployment. Device management remotely and securely allows functions such as firmware and software upgrades, security patch installations, factory resets, data wipes, device configurations, upgrades for new protocol support, and device lock functions, to name a few.

A real-world example of how device management can solve a problem is an IoT sensor programmed to report a block of information once per day, at exactly 5 a.m. when there is relatively little cellular traffic. But when thousands of such sensors were deployed in a small area, the crush of thousands of devices was sufficient to knock out part of the network to other users. A quick software upgrade that spread out the reporting was delivered via the device management platform, thus solving the problem.

Popular standards-based device management protocols include OMA-DM from the Open Mobile Alliance (OMA) and the TR-069 family of standards from the Broadband Forum. The recently published Lightweight Machine-to-Machine (LwM2M) standard from OMA stands out for addressing IoT. It is designed for "constrained" devices that have limited processing power, memory, and battery life while still meeting the requirements of more complex devices.

Key features of a device management solution include:

- Automated device configuration of on-device parameters including server addresses and communication protocols.
- Over-the-air remote firmware upgrades for devices that remain in operation for long periods of time.
- Remote reboots, diagnostics and troubleshooting to help eliminate costly truck rolls to device sites and to provide vital insights into device performance by remotely collecting diagnostic data.
- Security and integrity to ensure that device software is authentic, and data collected by the devices are not compromised.

One of the crucial influencing decisions for selecting a device management platform — apart from the ability to manage connected devices irrespective of protocol or transport channel support — is the ability to efficiently handle and manage firmware upgrades, and applications that enhance the device capability with newer features and security fixes. Another key criterion for selection is support for different deployment scenarios, such as traditional, automated, cloud-based, or hosted ones, which can significantly reduce total cost of ownership (TCO) and operating expenses.

Cities need to make certain that IoT devices deployed on their networks have an installed device-management client. A non-proprietary and open solution will ensure interoperability with device-management solutions at lower cost. A strong device-management solution is critical to ensuring data provided by the devices has not been

compromised — a crucial aspect of ensuring the success of a data exchange and a data marketplace.

For more detailed information, see Annex A.

Security Control and Trust

Trust in any connecting IoT device is the most critical element in any IoT Smart City data sharing platform. Without confidence in the source and usage policies of data generated from an IoT device that nourishes the Smart City Framework, data sharing will be constricted, and the integrity of the ecosystem will become suspect. That will undermine credibility of business decisions, and worst still, affect critical infrastructure.

Ensuring that IoT devices can be verified and that trust can be established ensures the integrity of IoT data. A vibrant data economy can then be created, fostering innovation that meets the unique needs of each municipality.

The landscape in an IoT Smart City consists of devices with dramatically different data integrity profiles:

1. Controlled IoT Devices — Water meters, energy management, etc., where the devices are installed, operated, and managed by the local municipality.
2. Contracted IoT Devices — Traffic lights, public transportation, CCTVs, etc., where the devices are installed operated and managed by an external party under a managed services contract with the local municipality.
3. Unknown and Uncontrolled IoT devices — Privately owned and managed devices that contribute data that could be beneficial to the municipality.

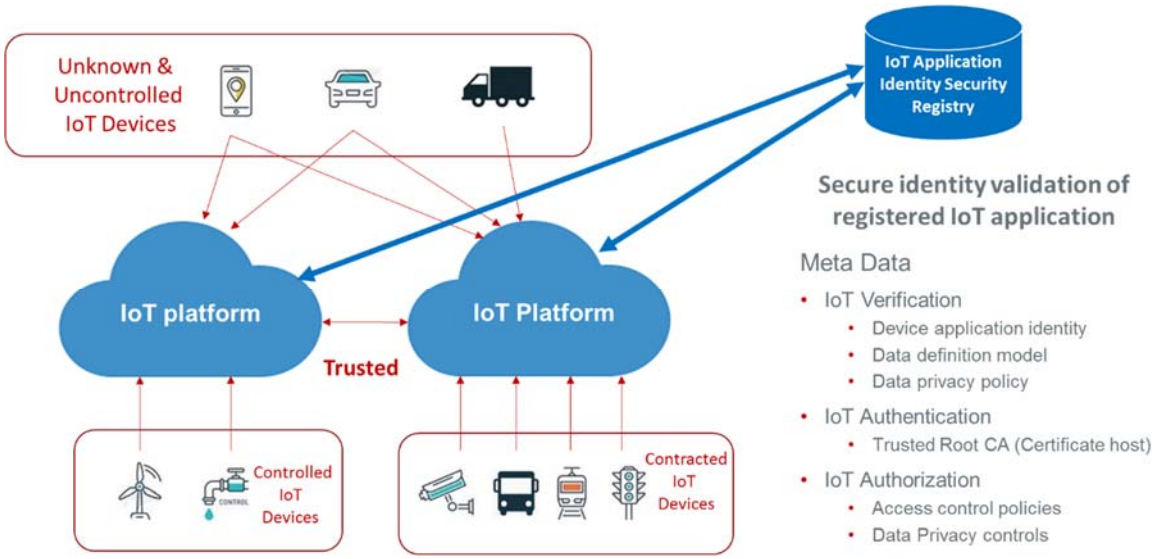
In all of these categories, knowledge of the capabilities of the IoT device's application is important in determining the extent to which the data it produces and shares can be trusted. Complicating the issue is the fact that multiple applications can be providing information via a specific device, and these applications may not share the same security characteristics. Controls over the IoT supply chain using sub-contractors, third-party services, or consumer connected things challenges the Smart City provider to know what is connecting and is it authentic and fit for its intended purpose. For many IoT applications-supporting industries such as healthcare, the Smart City, and critical infrastructure, device compromise can be a significant concern with potentially catastrophic consequences.

Identifying and authenticating an IoT device at the application layer is fundamental to ensuring the data can be trusted.

There are four important considerations that every Smart City must address to facilitate and encourage data sharing:

1. IDENTITY — What is connecting to provide the data?
2. AUTHENTICATION — Can the identity be trusted and verified?
3. PRIVACY — How, where, and when can the data be used?
4. ECONOMICS — What are the monetization considerations between data provider and data consumer?

Addressing these four considerations requires that a critical component of an IoT Smart City Data Sharing platform be an IoT application identity security registry. This registry can provide a central trusted repository of IoT application identities and profiles to enable IoT platforms to identify and authenticate IoT device application data from known trusted sources through an automated process. Such a registry provides the foundation for IoT security across the ecosystem for all stakeholders and ensures that IoT applications and the data they produce can be trusted. This will facilitate the sharing and commercialization of IoT data while protecting consumer privacy.



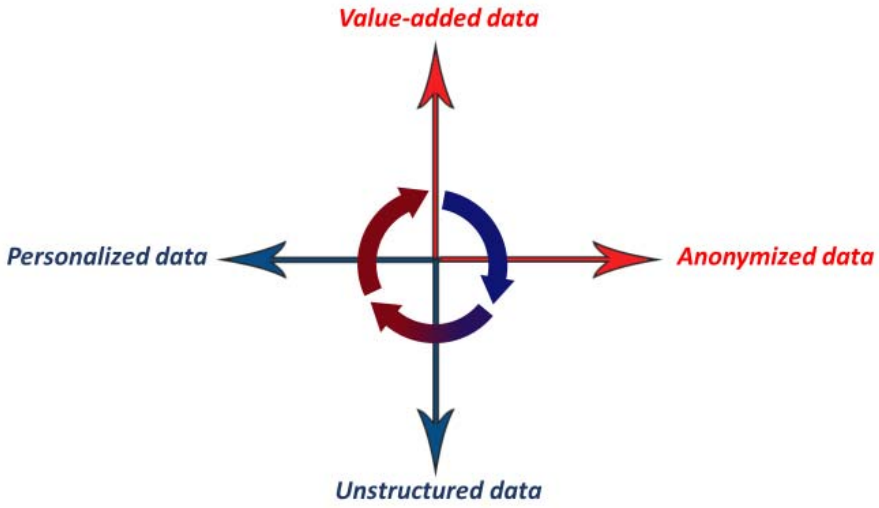
For device and application vendors, the IoT application identity security registry provides the ability for IoT devices to be uniquely identified and authenticated so they can be broadly adopted by any IoT service provider, increasing the addressable market

opportunity. The registry provides metadata regarding the characterization of the IoT device and the format of the data it produces, thus resulting in secure, trusted interoperability for integration with any appropriate application. The registry can provide metadata pertaining to the permissible use for the data generated by the IoT application and the constraints that should be applied for use and/or sharing of the data. All this enables applications to be compatible with a greater range of IoT devices, thereby improving cost effectiveness while enhancing the rate of innovation.

Privacy and Ownership

From a privacy control level, it is important to recognize that the type of data enabled by Smart City applications is fundamentally different from data that has been traditionally shared through city resources and open data obligations. First, data derived from new IoT sources, like smart parking, lighting, and transportation infrastructure, represents a sea change in the volume and context of information that will need to be processed, stored, and appropriately shared across a Smart City ecosystem. Second, raw data will be most often transitioned to information (that is created from source data), content (that is filtered and cataloged), and analyzed data (which infers an additional level of value and usefulness). In most cases, this level of information may go beyond the traditional definition of open data. An important consideration is how cities will accommodate this new data paradigm.

Many existing privacy frameworks specifically developed for Smart Cities have assessed this issue from a defined set of dimensions — the degree to which data is viewed as personal or anonymized or the level of data refinement (raw or value-added). While this approach provides valuable insight into the issue of privacy, it does not solve the fundamental challenge of how cities will apply privacy controls to data, information, and content within the legal framework of regulations and obligations. Therefore, it is important to recognize the close linkage between privacy and data ownership.



There are two dimensions for cities to consider in relationship to ownership issues. The first dimension applies to platform openness, which can range from neutral to restricted-access models. The neutral approach is analogous to a Data-as-a-Service exchange where data from multiple public- and private-sector sources might be made available to marketers (e.g., to target their customers). Conversely, the restricted-access model provides data access to a selected group of authorized users – for example, Social Security data provided to authorized branches of government.

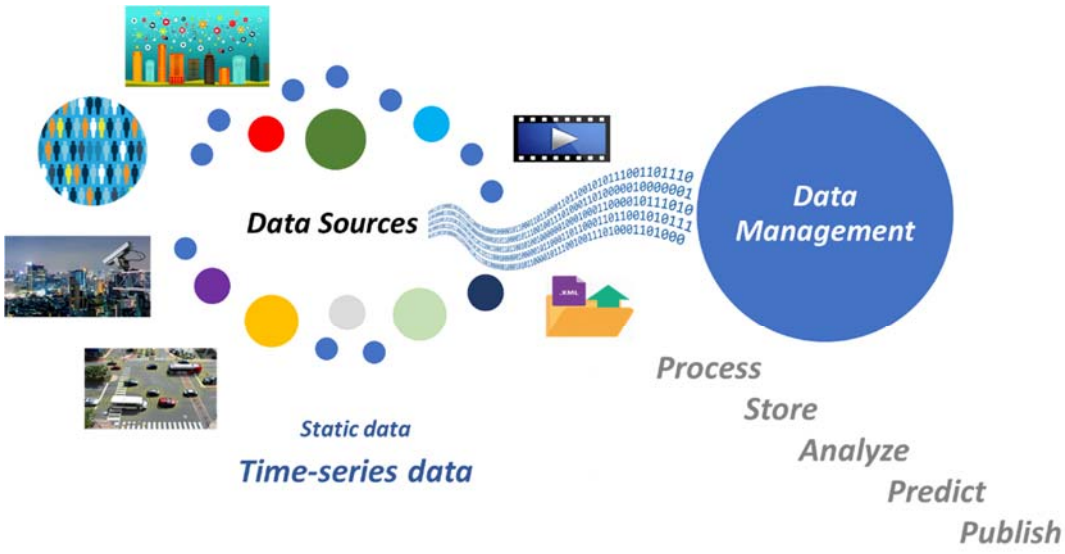
The second dimension to ownership applies to the data *per se*. It is possible to conceptualize three categories of data:

- 1st-Party Data — Data an organization collects on its own.
- 3rd-Party Data — Data provided by a 3rd party.
- 2nd-Party Data — Data an organization combines with data from a 3rd party provider in order to create derived value-added data.

The ability to combine different categories of data, some of which may originate from distributed data exchanges belonging to geographically dispersed agencies, is expected to provide new sources of value and enable service innovation.

Data Management

Data management acts as the core of any Smart City data platform. It relies upon data acquisition and collection from data sources to provide several stages of value enhancement, including: (1) data processing; (2) data storage; (3) analytics; (4) predictive actions; and (5) publishing. While all of these functions will ultimately support a Smart City operational vision, it is understood that real-time/predictive analytics platforms are still evolving in terms of large-scale deployments and advanced capabilities. Rapid market adoption of IoT devices is driving the development of data platforms that are optimized for treatment of time-series data, including centralized data management, edge management, and cloud-based solutions.



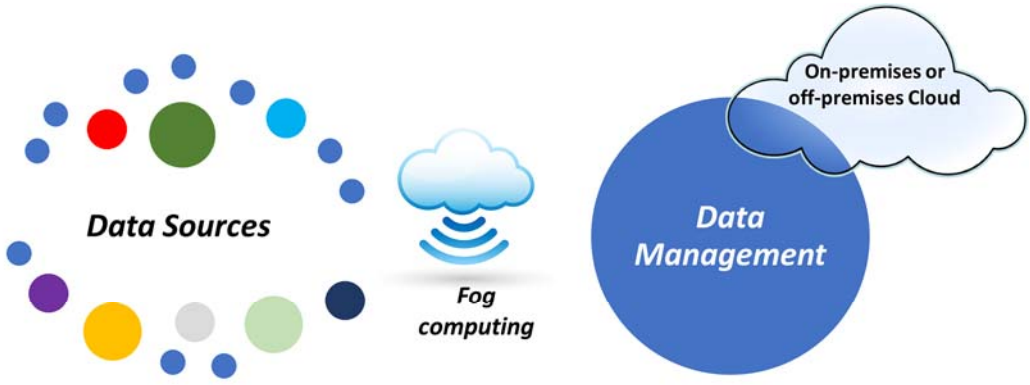
Smart City Data Management Ecosystem

Data management platforms provide lifecycle end-to-end ecosystem management of data, from collection to storage. At a fundamental level, data management must first address the complexities of processing and publishing multiple file formats, which are tightly coupled to the data sources that collect the data and the user community that applies the data to create applications and services. In addition, dependence on metadata will increase, as many Smart City applications require knowledge about the source of the information.

Data formats refer to the way in which data is organized within a file or dataset. The file types vary across a wide range of information and media types, including flat files, documents, images, video, hierarchical files, etc. While the data management component is somewhat transparent to the communication protocols, a key consideration of any data platform is the class of data protocols that must be supported by the architecture. The list of data protocols designed for IoT-sourced data and applications are extensive, including protocols such as CoAP, DDS, MQTT, Websocket, XMPP, and DSRC/C-V2X. For a table containing further details on these protocols, see Annex A.

Data management solutions can be implemented across a range of data infrastructure and cloud-based solutions, including on-premises cloud, hybrid cloud, and off-premises cloud platforms. These solutions offer the advantage of dense processing of information (such as batch data) and the ability to efficiently apply advanced analytics and deep learning techniques.

Alternatively, fog (or edge) computing solutions are beginning to impact the market, addressing the need for low latency and near real-time processing, storage, and analytics in cases where edge management of IoT data is critical to the application. This may include applications such as smart transportation, where low latency must be optimized and temporary storage of data at the edge is deemed appropriate. As Smart Cities begin to fully develop, it is expected that a combination of centralized processing and fog computing (from the perimeter of the data center to edge devices) will be the preferred solution for Smart Cities applications.



Fog Computing IoT Environment

One of the key challenges of any data management operation is the need for storage of

data at centralized servers or near the edge of the network. Applications that can execute near the edge, and rely on device-to-device or device-to-gateway communication, will typically trade-off the cost of bandwidth to centralized servers with the cost of edge storage. It is also important to delineate data from information or content. Raw data will often need to be structured to gather information, analyzed to create value, or delivered in the form of content. Traditional treatment of data storage is not necessarily applicable to the environment around time-series data, since the value of real-time data streams may only be several minutes or seconds versus the long-term needs of storing batch data.

Data analytics is a critical part of Smart City data management functionality, both from the ability to filter and take predictive actions, as well as the capability to create value on top of collected data. Within the bounds of a Smart City operating environment, analytics can function as the front-end to data integration among city agencies or can filter and compartmentalize data, such as data that is applicable to neighborhoods or more specialized needs within the larger community. Therefore, analytics must be assessed from the perspective of the underlying set of applications — large-scale analytics of big data that can take advantage of centralized processing (and scale) or edge analytics that requires proximity to the IoT edge devices and are dependent on low latency and location attributes. As predictive analytics become more mature in the market, machine learning and artificial intelligence will become powerful tools to migrate data management to predictive applications that increasingly rely on automation.

Most protocols being implemented for IoT today are based on publish/subscribe attributes. Publish/subscribe architectures are built on the premise that devices publish information to a group of data entities that subscribe to that subject of information, and those entities decide if the information is of value. An extension of this concept is the use of data brokers. In this scenario, IoT devices broadcast (or publish) information to data brokers who utilize subscriptions to trusted third parties that then share the information. These architectures represent a departure from telemetry-based polling solutions that routinely poll devices for relevant data. Conceptually, the data broker acts as an intermediary in a typical broadcast model, and is designed to optimize bandwidth and performance over a pure event-driven broadcast architecture.

Application and Service Layers

The roadmap to success for most cities will be manifested in the applications and services that define the Smart City vision. To be successful, the applications must be exposed to all the ecosystem participants: (1) the entities that operate the Smart City infrastructure; (2) the developers that will leverage the managed data to create valuable applications; and (3) the citizens that will utilize and benefit from innovative services and applications.

A Smart City application programming interface (API) is a pre-defined set of messages and scripts that allow developers to design valuable applications without the need to re-program the software components for each incremental application or service. An open API permits developers to publicly access specific aspects of the programming software which in turn allows applications to interact with the core programming software, as well as with other applications within a given API platform. While some degree of API development will drive the dashboarding of Smart City data and analytics within the city's departmental infrastructure, open APIs will enable use of Smart City applications for citizens and third parties delivering services.

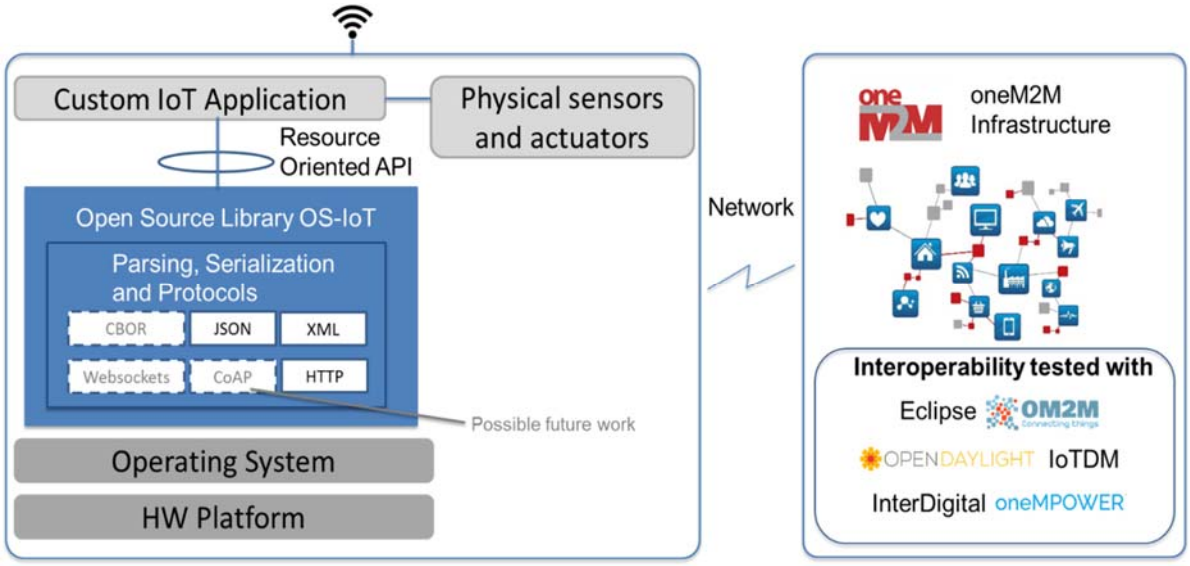
It is understood that some applications will remain within the city's operating structure and will not be exposed to developers or third parties (e.g., some aspects of public safety or other applications that may warrant appropriate privacy treatment). Some cities have already started to recognize the importance of creating an open API library to promote development of valuable applications. In that context, APIs may be developed in conjunction with a city's selected data management platform or may be independently developed to operate with that platform, but be managed as part of an API program that encourages commercial development of value-added applications with the private sector.

Several cities have begun to offer open data to citizens and businesses via open data portals. In addition, some Smart Cities are beginning to advertise a library of open APIs, often cataloged by city department or resource, to allow developers to design and make available a suite of applications that leverage open data. These API catalogs are sometimes hosted by the city or via third-party data portals.

One example of an open source client library for lightweight IoT devices is ATIS' new Open Source Internet of Things (OS-IoT) software library, which helps IoT app developers more easily connect their products to the open, interoperable oneM2M ecosystem. The

global oneM2M standard defines a common, interoperable platform for IoT systems, providing application-independent building blocks that fulfill the core tasks of data collection, management, and distribution needed by IoT solutions. By making it easier to support oneM2M in device software, OS-IoT is ideal for use by embedded application developers who want to participate in the oneM2M ecosystem to provide open, scalable, cloud-based IoT data collection and management. The OS-IoT library is seen as a critical resource in helping to boost oneM2M adoption for smart devices and other embedded applications.

Below is an illustration of the ATIS OS-IoT development scope:



Additional information can be found at http://os-iot.org/.

7. Standards and Industry Collaboration Activities

This section acts as a guide to a broad range of industry standards and collaborative activities related to Smart Cities and the integration of data and IoT-connected devices. The information in this section is not intended to characterize or make assertions about the work of each organization. Descriptions and references shown below have been obtained from information published by each organization.

ATIS

In addition to the Smart Cities initiative (outlined in this report), ATIS has a number of related projects and committees that impact the development of Smart Cities strategies and solutions. Some of these key activities include:

Open Source IoT

In September 2017, ATIS released the Open Source Internet of Things (OS-IoT) software library, which is designed to enable IoT app developers to more easily connect their products to the open, interoperable oneM2M ecosystem, reducing time-to-market and barriers to entry.

The OS-IoT library provides device-side (i.e., Application Entity in oneM2M terminology) support for fundamental oneM2M network and protocol functions, allowing application developers to interact with the system over a resource-oriented API. This frees developers to focus instead on the unique, value-added aspects of their applications. Learn more about the OS-IoT project at https://www.os-iot.org.

App-ID Registry

It is important to enable delivery of globally unique software application identifiers based upon oneM2M specifications and application identifier management in order to support developers and enterprises within industry verticals.

The oneM2M App-ID Registry solves the problem by providing a single source for application registrations and subsequent lookups. The registry enables:

- Generation of unique standards-based identifiers.
- Centralized App-ID data management through a robust, fault-tolerant registry.

- Processing of thousands of concurrent transactions.

ATIS, a oneM2M founding partner, is the Registry Management Authority for the oneM2M App-ID Registry powered by iconectiv. For more information, please contact appidregistry@atis.org.

To create an official, globally unique App-ID for your oneM2M compliant application, please click here.

Connected Car Cybersecurity

The ATIS Connected Car - Cybersecurity Ad Hoc fills a vital role in advancing industry-to-industry dialog between ICT experts and vehicle original equipment manufacturers (OEMs) for the purpose of improving connected vehicles' security. The group is analyzing the communications paths to the connected car, developing a cybersecurity threat model, and identifying potential solutions (i.e., network services that the ICT industry can offer). Its findings demonstrate that the ICT industry can be a valued partner to the automotive OEMs in terms of making connected cars more secure.

The report from this Ad Hoc can be downloaded at:

Improving Vehicle Cybersecurity: ICT Industry Experience and Perspectives

oneM2M

oneM2M is the global standards initiative for machine-to-machine communications and IoT. ATIS is a Founding Partner of oneM2M.

The purpose and goal of oneM2M is to develop technical specifications that address the need for a common M2M service layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide. A critical objective of oneM2M is to attract and actively involve organizations from M2M-related business domains such as: telematics and intelligent transportation, healthcare, utilities, industrial automation, and smart homes, to name a few. Initially, oneM2M shall prepare, approve and maintain the necessary set of Technical Specifications and Technical Reports for:

- Use cases and requirements relevant to a common set of service layer capabilities;

- Service layer aspects with high-level and detailed service architecture, recognizing an access-independent view of end-to-end services;
- Protocols/APIs/standard objects based on this architecture (open interfaces and protocols);
- Security and privacy aspects (authentication, encryption, integrity verification);
- Reachability and discovery of applications;
- Interoperability, including test and conformance specifications;
- Collection of data for charging records (to be used for billing and statistical purposes);
- Identification and naming of devices and applications;
- Information models and data management (including store and subscribe/notify functionality);
- Management aspects (including remote management of entities); and
- Common use cases, terminal/module aspects, including service layer interfaces/APIs between:
    - Application and service layers;
    - Service layer and communication functions

Additional details can be found at:

http://onem2m.org/

IEEE Standards Association (SA)

The IEEE supported the formation of a "Smart Cities Initiative" from 2013-2016, which is managed by the IEEE Power & Energy Society (PES) starting in 2017.

The IEEE Smart Cities Initiative is a global, multi-disciplinary effort to:

- Drive a top-down initiative where the IEEE worked directly with municipalities.
- Create a vibrant and world-wide network of cities, providing education, insights and expertise.
- Collaborate to share knowledge, experience and good practices.
- Involve local governance, universities, industries and local IEEE volunteers.
- Assist municipalities in managing the transition to urbanization.
- Raise awareness of the benefits and downsides of technology and help guide the appropriate uses of technology.

Examples of IEEE's Industry Connections Program include IEEE Open Data, IEEE Smart Cities Compliance Indicators, IEEE Digital Inclusion through Trust & Agency, and IEEE Big Data Governance and Metadata Management.

Additional information can be found at:

https://smartcities.ieee.org/

International Electrotechnical Commission (IEC)

The IEC provides International Standards and Conformity Assessment for all electrical, electronic and related technologies. The IEC Standardization Management Board agreed to set up a Systems Evaluation Group (SEG) on Smart Cities in June 2013. The mission is to foster the development of standards in the field of electrotechnology to help with the integration, interoperability and effectiveness of city systems. The group finalized a report recommending the setting up of a Systems Committee (SyC) on Electrotechnical aspects of Smart Cities in August 2015.

Additional details can be found at:

http://www.iec.ch/smartcities/

Industrial Internet Consortium

The Industrial Internet Consortium was founded in 2014 to bring together the organizations and technologies necessary to accelerate the growth of the Industrial Internet by identifying, assembling and promoting best practices. Membership includes small and large technology innovators, vertical market leaders, researchers, universities and government organizations.

The goals of the Industrial Internet Consortium include:

- Drive innovation through the creation of new industry use cases and testbeds for real-world applications;
- Define and develop the reference architecture and frameworks necessary for interoperability;
- Influence the global development standards process for internet and industrial systems;

- Facilitate open forums to share and exchange real-world ideas, practices, lessons, and insights; and
- Build confidence around new and innovative approaches to security.

Additional information can be found at:

http://www.iiconsortium.org/about-us.htm

International Telecommunication Union (ITU)

ITU-T Focus Group on Smart Sustainable Cities (FG-SSC) was formed under ITU-T parent group Study Group 5.

The FG-SSC acted as an open platform for smart-city stakeholders – such as municipalities; academic and research institutes; non-governmental organizations (NGOs); and ICT organizations, industry forums and consortia – to exchange knowledge in the interests of identifying the standardized frameworks needed to support the integration of ICT services in smart cities.
The FG-SSC concluded its work in May 2015 by approving 21 *Technical Specifications* and *Reports*.

http://www.itu.int/en/ITU-T/focusgroups/ssc/Pages/default.aspx

The work on SSC is being continued by the new ITU-T Study Group 20 on "Internet of things (IoT) and smart cities and communities (SC&C)", which provides a unique platform to influence the development of international IoT standards and its application as part of urban-development master plans. This Study Group provides IoT standards developers the opportunity to target their standardizations efforts towards specific applications and various urban parameters, thereby responding to the requirements of standards implementers including city administrations, energy and water utilities, healthcare providers, and transportation authorities.

http://www.itu.int/en/ITU-T/about/groups/Pages/sg20.aspx

International Technical Working Group on IoT-Enabled Smart City Framework

Two barriers currently exist to effective and powerful Smart City solutions. First, many current Smart City ICT deployments are based on custom systems that are not interoperable, portable across cities, extensible or cost-effective. Second, a number of architectural design efforts are currently underway (e.g., ISO/IEC JTC1, IEC, IEEE, ITU, and consortia) but have not yet converged, creating uncertainty among stakeholders. To reduce these barriers, the National Institute of Standards and Technology (NIST) and its partners are convening an international public working group to compare and distill (from these architectural efforts and city stakeholders) a consensus framework of common architectural features to enable Smart City solutions that meet the needs of modern communities.

https://pages.nist.gov/smartcitiesarchitecture/

This activity includes working groups covering:

- *Application Framework* – Document the scope of Smart City applications and metrics
- *Consensus PPI* – Determine "Pivotal Points of Interoperability" that multiple smart city technologies share in common
- *Deployed PPI* – Discover and document actual Smart City deployments which make use of two or more different technologies and are integrated using Pivotal Points of Interoperability

LoRa Alliance

The LoRa Alliance was initiated by industry leaders with a mission to standardize Low Power Wide Area Networks (LPWAN) being deployed around the world to enable Internet of Things (IoT), machine-to-machine (M2M), Smart City, and industrial applications. Alliance members collaborate to drive the global success of the LoRa protocol (LoRaWAN), by sharing knowledge and experience to guarantee interoperability between operators in one open global standard. LoRaWAN™ is a Low Power Wide Area Network (LPWAN) specification intended for wireless battery-operated Things in a regional, national or global network. LoRaWAN targets key requirements of IoT such as secure bi-directional communication, mobility and localization services.

Additional information can be found at:

https://www.lora-alliance.org/

Open Connectivity Forum

The Open Connectivity Forum (OCF) is dedicated to ensuring secure interoperability for consumers, businesses and industries by delivering: a standard communications platform; a bridging specification; an open source implementation; and a certification program, allowing devices to communicate regardless of form factor, operating system, service provider, transport technology or ecosystem. OCF's specifications leverage existing industry standards and technologies, provide connection mechanisms between devices and between devices and the cloud, and manage the flow of information among devices, delivering a single solution covering interoperability across multiple vertical markets and use cases.

Additional information can be found at:

https://openconnectivity.org/

Smart Cities Council

The Smart Cities Council provides readiness guides, financing templates, policy frameworks, visibility campaigns and regional networking events that promote the following core principles:

- *Livability:* Cities that provide clean, healthy living conditions without pollution and congestion; with a digital infrastructure that makes city services instantly and conveniently available anytime, anywhere.
- *Workability:* Cities that provide the enabling infrastructure — energy, connectivity, computing, essential services — to compete globally for high-quality jobs.
- *Sustainability:* Cities that provide services without stealing from future generations.

Additional information can be found at:

https://smartcitiescouncil.com/article/about-us-global

US Ignite

US Ignite spurs the creation of next-generation applications and services that leverage advanced networking technologies to build the foundation for smart communities, including cities, rural areas, regions, and states. US Ignite programs include:

Smart Gigabit Communities

This program accelerates the development of advanced gigabit applications that cannot run on current networks as the bedrock of smart communities by identifying new economic and social opportunities created by those applications. US Ignite believes that the communities most likely to become the first smart communities are those with widespread, open, and flexible advanced networks.

https://www.us-ignite.org/programs/smart-gigabit-communities/

Global Cities Team Challenge (GCTC)

NIST and US Ignite have created the Global City Teams Challenge (GCTC) to serve as a platform for local government representatives and technology solution providers to develop solutions designed to address vexing municipal problems with Smart City applications.

https://www.us-ignite.org/programs/global-city-teams-challenge/

8. Evolution to Data Marketplaces

From a technology standpoint, data exchanges will become commonplace because of the potential of having a single access point from which to make many different forms of IoT data available. There are also economic benefits that come with sharing implementation costs.

The next evolution for data exchanges will be to augment their power with capabilities that support higher-value data sharing relationships across multiple user groups. This would happen through innovative business models.

There are several aspects to this evolution, some of the most important of which are issues related to technology. An effective data exchange will accommodate data from different connected device and sensor sources and numerous communications and connectivity protocols. Such a data exchange would be attractive to the user community because it would promote technology-neutral solutions.

A second important aspect to consider is collaboration among multiple organizations. This could occur, for example, in a complex manufacturing chain or a multi-party, Smart City environment. Regardless of the type of entity, the task of managing a data exchange must focus on simplicity so that technology and service provider partners can readily join the exchange and so that individual exchanges can eventually interact with other exchanges.

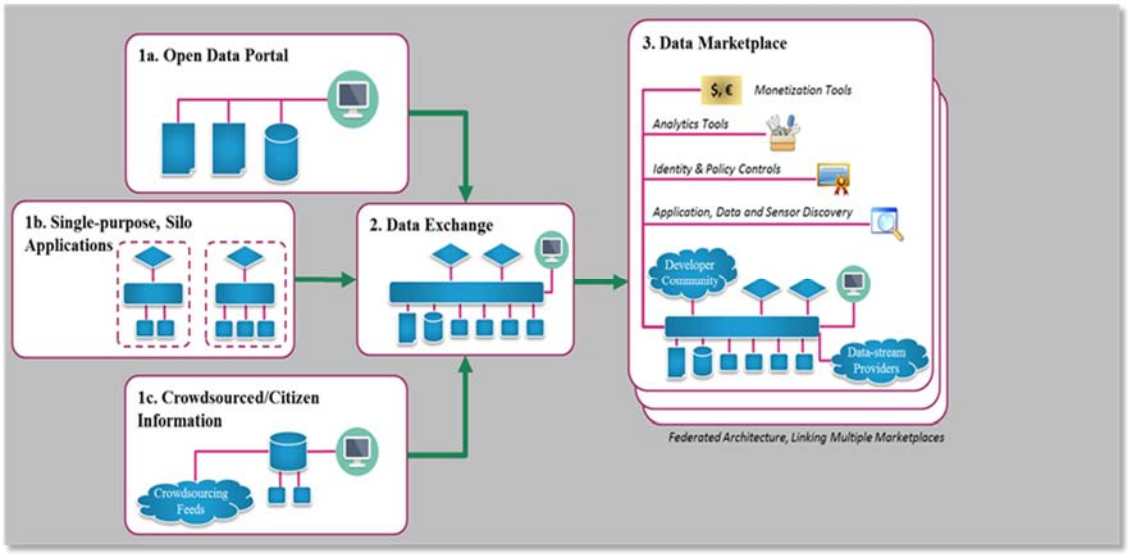
A third aspect to consider is the creation of a set of marketplace enablers designed to support commercial trading of data and applications. These service enablers would include the underlying tools that help realize QoS objectives such as data availability and refresh rates.

Commercialization Requirements Will Drive Demand for Marketplaces

Early-stage Smart City applications focus on point solutions in areas such as smart parking, intelligent public-transport or dynamic street lighting. There is a parallel trend for some cities to expose in-house data in response to freedom-of-information requests and the need to increase transparency to citizens. These trends are often a launchpad for more innovative methods of delivering citizen services.

As the scope of these types of activity grow, cities look for scale economies to manage implementation and end-user costs. The introduction of shared technology, such as cloud hosting and common data-access interfaces, is a starting point for a data exchange.

The open data portal (1a) and single-purpose silo applications (1b) illustrated below show how different organizations are likely to embark on the journey: first to create a data exchange (2) and then to participate in a data marketplace (3).



Evolutionary Roadmap to Data Marketplaces

The concept of a data exchange evolves to a data marketplace once there is an inclusion of value-added data management capabilities. Examples include: a toolkit of common analytics functions; service enablers relating to access, privacy, security, and usage controls; monetization capabilities; and visualization and resource discovery tools.

These are fundamental elements of a data marketplace, as data owners should be able to offer access to their data — on technical and commercial terms — to a variety of data consumers. These "consumers" may be specialist software firms that process raw data and package it for use by application developers. There may be firms that wish to monitor their own assets or service providers that require access to one or more data streams in order to offer a "connected-service".

Profile - Data Marketplace	
Solution Characteristics	• Supplements data exchange with capabilities to involve third-parties with support for data licensing models. • Third-parties can be other cities in a federated operating model.
Incremental Value-add	• Fosters an ecosystem of private sector specialists (applications, data management, innovation, etc.). • Includes features that enable the marketplace to exist (data rights, data trading, etc.). • Engenders federation, bringing Smart City solutions within economic reach of small/medium-sized cities.
Limitations	• Relies on an open- ecosystem operating model and a higher level of operational complexity.

Implications for data marketplace implementation

Large organizations will implement data exchanges for their own applications and attempt to break through organizational silos. Doing so may be a sizeable undertaking, especially in the case of large organizations comprising multiple departments or lines of business.

Situations that require large businesses exchange data with their partners (e.g., suppliers, business and consumer customers, regulators) will necessitate open APIs and shared database techniques (e.g., as in the case of Blockchain ledgers) in order to simplify technical integration.

Identity management and authentication will be critical elements, as they ensure trust among ecosystem participants and to lower the barriers to entry for new entrant data-management service providers.

In due course, individual data marketplaces will seek to collaborate in a federated architecture. An illustration of this model would occur in the Smart City arena if one city — for the purposes of performance benchmarking, for example — wishes to share data with other cities in distant regions.

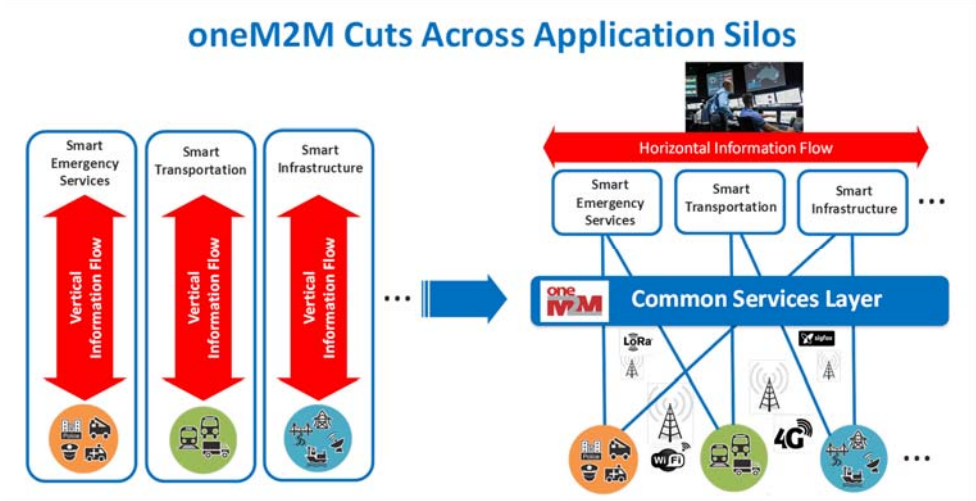
This model carries over equally to applications and solutions built for one location, which may be exported for use in another location. These marketplace examples, relating to the trade of data and applications, demonstrate the benefit participating cities could realize through the sharing of knowledge, best practices, and development costs.

To achieve interoperability in technical, access-control, and data interoperability domains, individual marketplaces will need to agree on a set of interoperability standards, such as those maintained by the oneM2M Partnership Project.

Overview of the oneM2M™ Standard

oneM2M is a standard for common service enablers (e.g., device management, communications and data management, resource discovery, security, semantics) in a horizontal IoT platform. It functions as a middleware layer between applications and the underlying networks that connect individual devices, gateways, and sensors.

One consequence of individual applications sharing these common services is to allow previously siloed and vertical applications to cross-communicate effectively, reliably and securely in a multi-application environment.



Technology abstraction and interoperability are core principles of the oneM2M platform architecture. As a middleware item, the abstraction concept inherent to oneM2M's common service layer shields users and application developers from the connectivity and remote management complexities associated IoT devices and sensors. It also makes new service and business opportunities possible by allowing applications to share resources and data.

Wider adoption of standards-based solutions for data exchanges and marketplaces will help users, who will benefit from a large ecosystem of solution providers and costs that are influenced through greater competition.

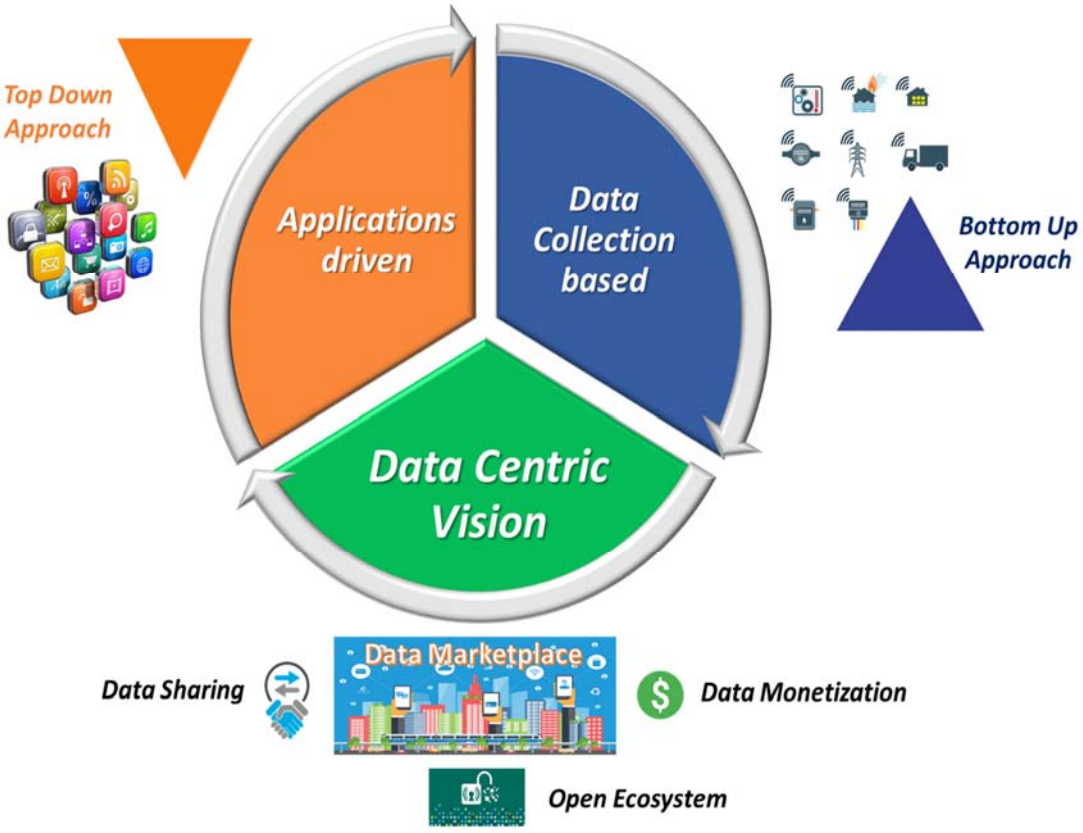
Standardization will also reduce the risk of vendor lock-in while promoting interoperability capabilities that allow individual marketplaces to effectively interact with one another.

9. Recommended Steps for City Planners

The purpose of this report is to promote a robust and extensible data- sharing strategy that meets each Smart City's unique vision. While this suggests a myriad of different Smart City planning strategies, there exists a set of common steps that will support any city's data evolution plan. The following four recommended steps offer Smart City planners a tool kit for evolving a Smart City from an integrated data platform to a long-term data management strategy.

1. **Start with a *data centric vision* that incorporates applications and data collection, while focusing on an evolutionary path to a data marketplace**.

Many approaches exist today as a starting point for Smart City design. Application-focused approaches generally take a "top-down" view, starting with a unified platform that allows the consistent execution of a wide range of city and citizen applications. Alternatively, a data collection-based approach is a "bottom-up" model that utilizes a city's core data platform and edge management capabilities to efficiently process, store and analyze information collected by data sources. While both solutions are relevant and viable, it is recommended that cities consider a strategy that supports the unification of these approaches with a data-centric vision that can progress a city to a data marketplace.



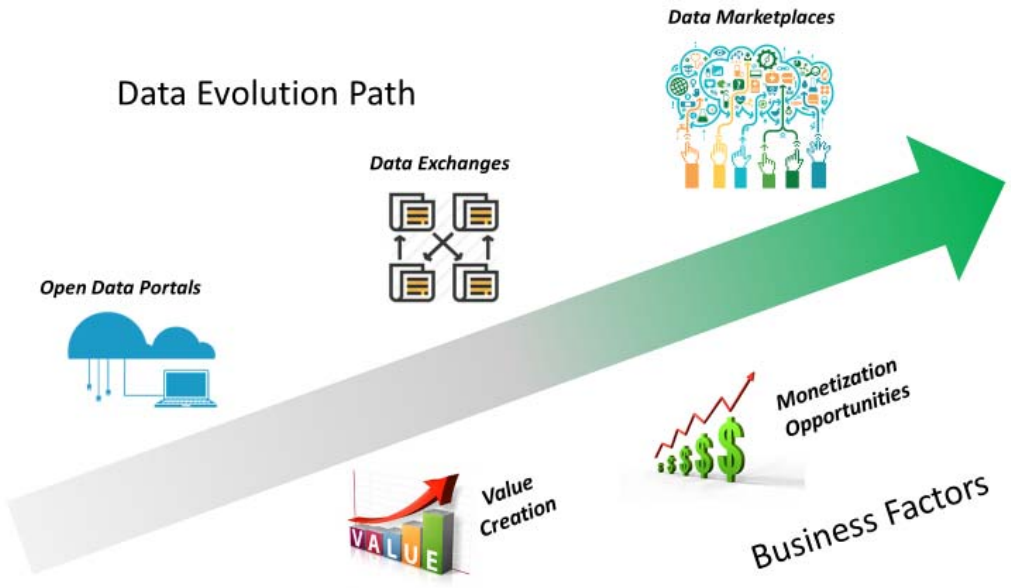
The following is a list of the most critical actions to take in developing a data-centric solution:

- Create an approach that can take advantage of large-scale processing and analytics at the core, yet leverages edge management for applications that require real-time processing, low latency and limited needs for storage.
- Design data resiliency into the Smart City infrastructure, which may include core and distributed resiliency, and resiliency plans with other cities.
- As more sources of data emerge, both within a city infrastructure and citizen crowdsourced scenarios, leverage data analytics to optimize the collection, filtering and utilization of data.
- Incorporate a consistent approach to identity management, authentication, authorization, security and trust across the data platform and the data sources; consider current standards-based approaches (e.g., oneM2M).
- Develop a plan that progresses an open data portal approach to a longer-term open API library for application developers.

- Early in the planning approach, identify the constraining factors that must be addressed, such as privacy, ownership, usage controls, and other legal and business issues.

2. Create a strategy that allows evolutionary steps from a data integration approach to a data exchange, and ultimately to a data marketplace.

Cities that embrace the vision of a robust data marketplace will need to create an evolutionary plan that maximizes investments and enables re-use of the data platform infrastructure. Many cities are appropriately focused on an integrated data approach (optimized for inter-departmental sharing coupled with an open data portal) in the early stages, where data can be leveraged across many city departments and shared with citizens through an initial set of valuable applications. The challenges associated with creating a city data exchange are most often related to a combination of business, technical and data ownership issues. As cities evolve to a citizen-facing data marketplace, additional business and privacy issues will need to be assessed and addressed in advance.

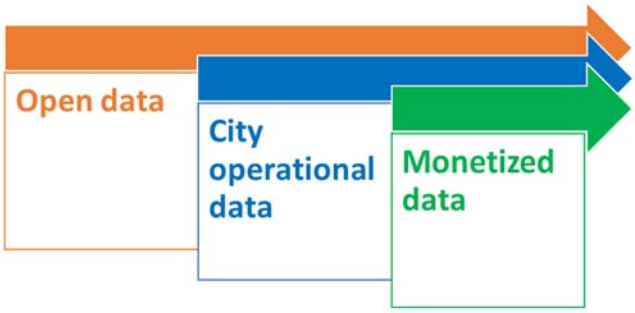


In considering a long-term data management strategy, cities will need to consider the timing and requirements associated with each stage of the migration path to a data marketplace solution. While the open data portal stage may improve efficiencies and offer greater transparency, there will be limited value creation in this environment. The

evolution toward a data exchange does apply additional analytics and allow transfer of data between cities or trusted parties, but limitations regarding citizen-facing application development and monetization will still exist at this stage. From a business perspective, it is possible that cities may embark on a different business structure in support of a data marketplace, as partnerships and federated solutions may become more prevalent.

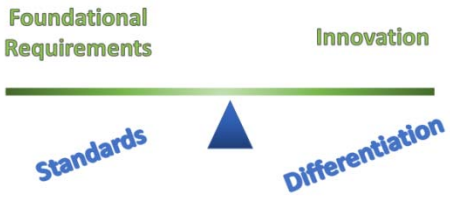
3. Recognize the importance of monetization as a critical element of maintaining the sustainability of a Smart City.

It is acknowledged that monetization is a business concept that has traditionally fallen outside of city operating budgets and decision-making. The concept of monetization should not be confused with open data obligations. Cities will continue to provide open data services to citizens and businesses in the normal course of sharing access to collected data. The ability to monetize data is most often related to the city's ability to take the actions required to add value to the data, whether through city-owned platforms or through partnerships with trusted third parties.



Monetization of data should be applied in a targeted manner as monetization cannot be applied across all data collected and processed by a Smart City. A willingness to pay for data is most often focused on application developers (who in turn create value) or third parties that will use treated data to generate additional value across many users. Therefore, monetization will be tightly coupled to the ability to create data marketplaces in the future. Monetized data most often falls outside the boundary of open data portals and data exchanges. It infers that cities act upon data to create value, or agree to share data with third parties or federations that then combine city data with other available data or data analytics in order to create value. It is expected that many cities will adopt monetization in the future as a pathway to expansion of Smart City capabilities beyond a core set of needs. At a minimum, it will be important for cities to develop a future monetization plan that capitalizes on early investments in Smart City infrastructure as opposed to stranding investments.

4. Adopt a view of data sharing as an asset, and therefore undertake the necessary steps to treat the exchange of data in a consistent and interoperable model.



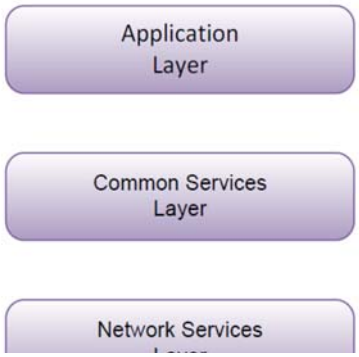
Cities should recognize the inherent benefits of exchanging data in a consistent manner, and where possible, through a standards-based model that encourages data sharing with citizens, trusted third parties and other local/state and federal government entities. Consistent data sharing does not prohibit the deployment of a broad range of data platforms within a city's infrastructure, but it does require that cities recognize the functional areas of data platform design that should be aligned across city platforms. Standards development organizations have long recognized the need to develop the foundational aspects of emerging technologies so as to promote interworking, while also allowing innovation on top of foundational agreements.

It may not be possible to standardize all aspects of Smart City deployment, but it is important to recognize the benefits of a consistent approach to data sharing in support of the evolution toward Smart Regions and city-to-city exchanges of data. Cities are encouraged to leverage the work of leading standards development organizations, and they are encouraged to create blueprints for interoperable data-sharing architecture. They should identify the foundational requirements that best promote innovation and the creation of real value to their citizens. ATIS' diverse membership, knowledge of ICT-based developments, global partnerships, and willingness to partner with cities in the data-planning stage can lay the groundwork for an open standards-based approach for addressing critical challenges and goals. Smart Cities and communities can benefit from a collaborative approach that allows interworking of elements, replication of good solutions, and innovation for citizens.

Annex A

Discovery

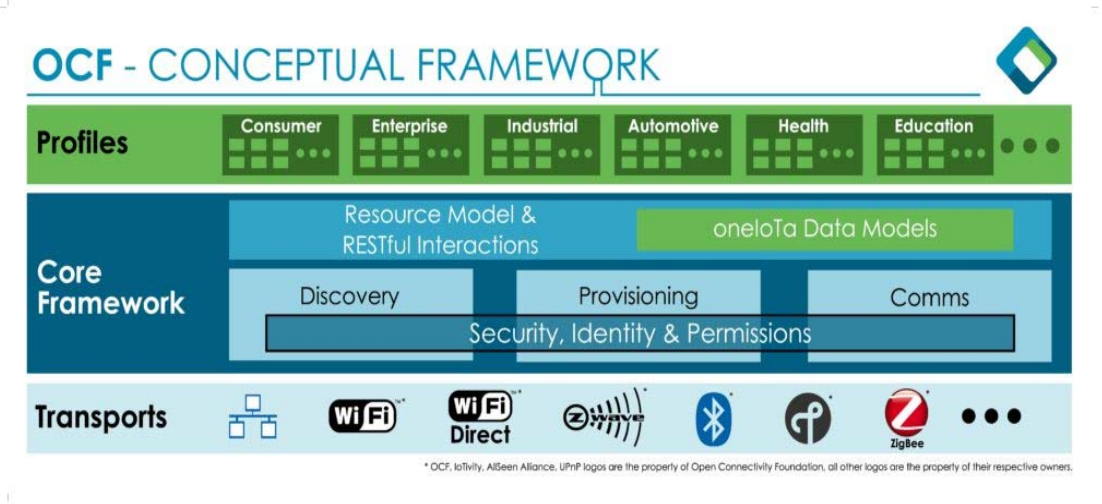
oneM2M treats discovery as part of a Common Services Layer function, where the originator of a request applies filter criteria (e.g., keyword, location, semantics) to search for information about services and applications contained in attributes and resources. The result of a discovery request is subject to access control policies associated with the M2M Service Subscription. A successful request is fulfilled with the discovered information about matching resources, which would typically include the address of the resourced device. Based on established polices, the information can be forwarded to other registered entities.



oneM2M Layered Model

The specifications developed by oneM2M include architecture, requirements, protocols, and syntax for resource discovery, content-based discovery, and semantic and on-demand resource discovery request. As part of the oneM2M specifications, details are provided for interworking with other technologies, such as AllJoyn, BBF, OMA, and 3GPP. Additional information regarding oneM2M is provided in Section 7 of this document.

The Open Connectivity Foundation (OCF) is establishing the necessary interoperability standard for connected devices, enabling them to discover and communicate with one another, regardless of manufacturer, operating system, chipset, or physical transport. OCF is focused on advancing IoT market needs by creating secure device discovery and connectivity, including the development of a core OCF Interoperability Specification. OCF specifications define both endpoint discovery and resource discovery.



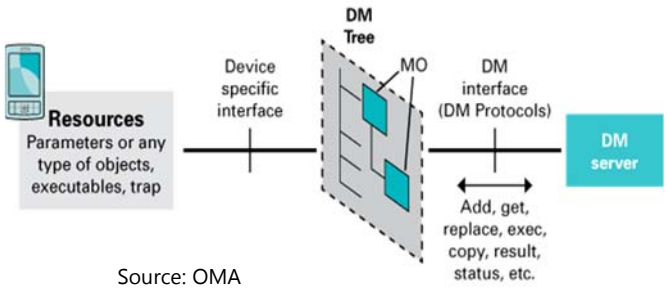
Endpoint discovery specifications support both transport protocol and HTTP discovery mechanisms, and describe how an endpoint is discovered by another endpoint, using multicast techniques. When the other endpoint is already known, endpoint discovery is not required.

OCF provides for resource discovery using three mechanisms: direct discovery (resources published locally at device hosting the resources); indirect discovery (resources published at third party assisting with discovery); and advertisement discovery (resources remote to the devices that are publishing discovery).

OCF has published a Core Framework Specification, which includes core architecture, core features, and protocols to enable OCF profiles implementation for IoT usages and ecosystems. This includes mapping to/from AllJoyn interfaces. OCF had previously acquired the assets of the UPnP Forum.

Device Management

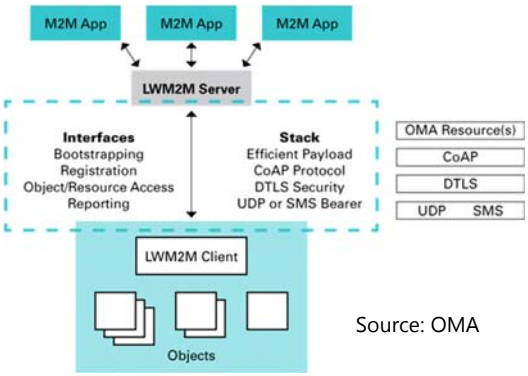
The Open Mobile Alliance (OMA) has developed two protocols for managing a large base of IoT devices. OMA-DM is HTTP/XML based approach that was originally developed for managing mobile devices like smartphones, tablets, etc., between a server and any number of client devices. OMA-DM was designed to



Source: OMA

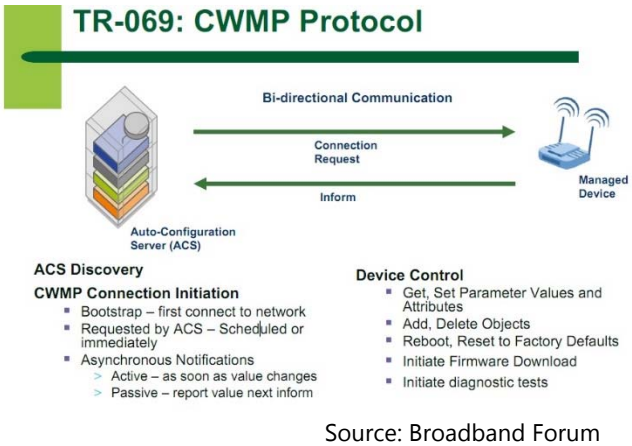
emulate the characteristics of mobile connected devices (constrained bandwidth and memory), but it was developed to operate over the wide range of communications and data transport media types. OMA-DM uses a command structure to deliver configuration parameters to a secured client device. This allows the server to manage parameters, perform troubleshooting and apply S/W updates, as required.

More recently, OMA has developed a LWM2M device management protocol intended to address the M2M market. This approach acknowledges the device and network resource constraints associated with IoT sensor devices. LWM2M is built on-top of CoAP and is object oriented, where each object has a unique identifier. It utilizes a data model to deliver device management and service establishment functionality to IoT devices. The common management attributes of LWM2M are: create, retrieve, update, delete and configure. LWM2M is designed for UDP and SMS transport layer support.



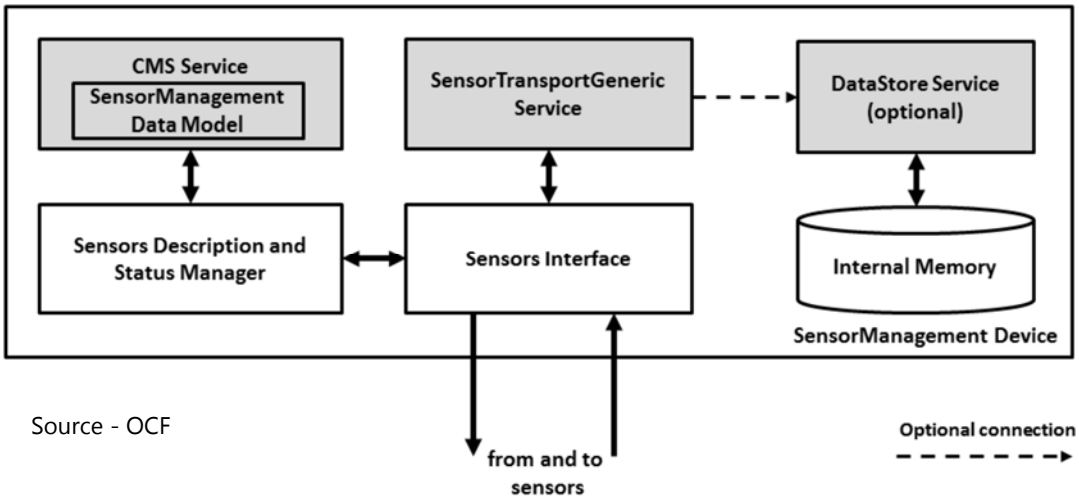
Source: OMA

TR-69 CPE WAN Management Protocol (CWMP) was developed by the Broadband Forum as an application layer CPE configuration protocol for use over IP networks. It was originally intended for home and business CPE devices like VoIP devices, set top boxes, routers, modems, etc. It relies on the presence of an auto-configuration server providing remote management and automatic configuration of CPE devices. Remote management functions supported by TR-69 include service activation, remote subscriber support, firmware updates and remote diagnostics. TR-69 CWMP has achieved wide adoption across the home CPE market, but its application across a broader range of IoT devices is still undetermined at this time.



Source: Broadband Forum

The UPnP Forum (now part of OCF) has developed the Device Control Protocol (DCP) specification covering basic management, software management and configuration management of home networked devices. It is an HTTP/XML based protocol that treats sensors and actuators as generic data sources, without detailed knowledge of the sensor's operation or underlying access network. Sensors are treated as a set of uniform resource names (URNs), and manufacturers can utilize the list of generic URNs to create their own sensor types. These specifications are generally targeted to the home IoT device market.



Source - OCF

Data Management

Protocol	***Description***
Constrained Application Protocol (CoAP)	A client-to-server low overhead lightweight protocol that is aligned with web protocols but designed for low power IoT device applications. It is a simple request/response protocol, developed to communicate over the Internet, operating over UDP. In general, CoAP is optimized for persistent monitoring of sensor data.
Distribution System for Real Time Systems (DDS)	A middleware protocol for publish/subscribe applications, optimized for heavily data-centric needs where contextual information can enhance the publishing and sharing information. It is generally applied as a device-to-device protocol for M2M communication.

Protocol	***Description***
Message Queue Telemetry Transport (MQTT)	An open source protocol solution for lightweight IoT clients. It supports publish/subscribe messaging for server-controlled IoT networks and supports broadcast applications. MQTT-S is designed for operation over UDP (instead of TCP). In general, MQTT is optimized for event-driven applications.
Websocket	An HTML5 bidirectional protocol that operates over TCP for real-time, event-driven applications. Part of HTML5 set of specifications, supporting web-based full duplex client-server functionality, that requires Websocket client and browser to be installed on the IoT device and related Websocket library at server. Accordingly, it does require HTTP implementation on the IoT clients.
Extensible Messaging and Presence Protocol (XMPP)	A protocol that was originally designed for instant messaging applications, without the need for a centralized server. Its extension to IoT supports addressable delivery of XML data for lightweight IoT devices like home appliances and retail-based devices. It can support both publish/subscribe and request/response architectures.
DSRC/C-V2X	Dedicated Short Range Communications (DSRC) and Cellular Vehicle to Everything are FOG based Peer-to-Peer protocols being proposed for vehicle-to-vehicle safety and event messages and providing detailed information about the vehicles operations (Latitude, Longitude, Speed, Direction, etc.) as well as critical events generated from the vehicle (Air Bag Deployments, Hard Braking, Emergency Alerts). This information, along with data generated by other sensors in the network, can be utilized by a wide range of Smart City/Smart Transportation applications and services.