Fostering inter-operable urban ecosystems through the adoption of common frameworks

Luis Diez, Ignacio Elicegui, Luis Sánchez, and Luis Muñoz,
University of Cantabria. Santander 39005, Spain
Email: {ldiez, ielicegui, lsanchez, luis}@tlmat.unican.es

***Abstract*—Worldwide cities are involved in a digital transformation phase. More sustainable cities and improving citizen's quality of life are the *leit motiv* of such transformation. However, such aims are difficult to achieve if the migration of the urban processes are not carried out following a common approach. Optimizing the behavior of any specific urban service needs to be performed taking into consideration both the service itself as well as its interaction with adjacent services. This means that any solution aiming to achieve the autonomous city management paradigm is tightly related to the adoption of common frameworks which are able to guarantee interoperability with other systems. Furthermore, cities themselves are not isolated systems. Well the opposite, cities interact one to the each other depending on different attributes. This implies that sooner or later optimizing some processes in one city without having in mind the adjacency to others might not be efficient enough. Hence, interoperability among cities will become a must, not just in terms of optimization but also replicability. Based on this boundary conditions this paper describes a framework aimed to ensure interoperability and replicability among cities. Some of the tools for assessing compliance with specific standardization activities are also presented.**

I. Introduction

Internet of Things (IoT) is reaching a maturity level which fosters its adoption in most of social, economic and industrial activities. In particular, urban ecosystems have understood that improving the citizens quality of life and reaching sustainability convey the adoption of disruptive technologies which enable to ubiquitously monitor the different subsystems and corresponding processes being executed in the cities. While in many cases proprietaries and standalone solutions are adopted, such an approach hinders the interoperability among different verticals (energy, traffic management or public transportation) and so the integration of heterogeneous data coming from them, to generate value-added information. It is in this context that the adoption of a reduced number of well-established interoperability points as well as common data models configures a promising approach for overcoming such constraints. Furthermore, it becomes also essential to provide ways to validate such interoperability points.

In the last years, some smart city architectures have been postulated seeking to respond to the urban challenges. However, none of them combine the features sought for interoperability and data exploitation. For instance, the ESPRESSO project [1] promotes common metadata structures and open standards to avoid vendor lock-in. However, it does not consider either data exploitation policies or systematic interoperability assessment. BIG-IOT project [2] also aims integration and interoperability, but the proposed architecture is not agnostic of the underlying IoT infrastructure, so hindering service replicability. Other projects, like symbIoTe project [3] or FIESTA [4], focuses on providing uniform data access by means of abstractions layers, hence they do not respond to the data exploitation need.

At the same time, we are witnessing different initiatives from standardization bodies to fulfill the mentioned requirements. The ITU-T Focus Group on Smart Sustainable Cities (FG-SSC) [5] proposes a basic reference architecture for smart cities embracing application layer, data and support layer, network and sensing layer. Similarly, the ISO/IEC JTC1 study group on Smart Cities [6] provides a layered smart city architecture also considering business aspects. In particular the following layers are defined: business layer, data layer, cloud and network layer, sensing layer and security layer. Another layered architecture is proposed by the AIOTI [7], embracing application, network and IoT layers. AIOTI seeks standardization, interoperability and policy issues for economic development and growth of digital markets. Furthermore, the ITU-T Focus Group on Data Processing and Management to support IoT and Smart Cities and Communities (FG-DPM) [8] defines the road-map for data access and management. Finally, the U4SSC [9] initiative, coordinated by ITU and UNECE, advocates for public policies that allow using ICT to facilitate transition of smart and sustainable cities.

Inspired in the previous initiatives, the SynchroniCity project aims to fulfill the aforementioned requirements by defining a set of minimum interoperability mechanisms and tools to validate them. Precisely, in this paper we describe such validation tools, that provide a certificate for service replicability.

The paper is structured as follows. Section II describes the SynchroniCity framework, highlighting its main components. Then, the interoperability validation methodology is described in Section III, and a practical deployment is described in Section IV. Finally, Section V concludes the paper outlining the future work and exploitation of the validation tools.

II. Adopting a Common Framework

When addressing interoperability and service replicability, some initiatives have taken a clean-slate approach, thus proposing new brand interfaces and procedures. However, this approach is likely to hinder the adoption of such new architectures by already deployed infrastructures. Opposed to that, the SynchroniCity project opts for defining a set of minimum interoperability requirements. In addition, in order to facilitate the integration and acceptance of the system, it is

TABLE I. STANDARD ADOPTION FOR FUNCTIONAL REQUIREMENTS

Functional requirement	Standard
Context Information Management	OMA NGSI/ETSI NGSI-LD
Data Models	FIWARE data models
Authorization	OAuth 2.0
Data market Place	FIWARE/TM Forum Business API

necessary to make use of public, and vendor neutral, standards and specifications. The use of standardized APIs facilitates the service implementation re-usability, thus fostering replicability. In addition, open standards ensure that the platform keep technologically neutral and avoid vendor lock-in issue. In the following we describe the the interoperability requirements and indicate the adopted standard for each of them, which are summarized in Table I.

A. Data management

As for data assets, the system is to provide means to track updates in the data in order to keep the services aware of such changes. Furthermore, considering the heterogeneity of the urban data, APIs are to provide searching functionalities based on multiple criteria, and with high granularity level. In addition, the platform should be also able to provide data storage capabilities. In this regard NGSI has been adopted to provide data context information. Although, OMA-NGSI [10] is taken as initial definition, the ETSI-CIM working group [11] has elaborated a new standard that incorporates linking data to the existing OMA-NGSI definition. This new standard will be adopted once it is fully defined.

Furthermore, an interoperable platform must ensure that the retrieved data is predictable, to ensure service replicability. In this regard, it is of utter importance that data-models are well defined for each kind of data asset. SynchroniCity leverages the data-models defined by the FIWARE initiative [1], and has defined new ones based on actual needs of cities[2].

B. Data marketplace

In order to exploit data, the platform is required to provide means to decide and enforce how and with whom data is shared. In this sense, the data market place has to let data providers to define access policies based on both the particular data assets and the data consumer. In addition, considering the growing importance of data, such marketplace needs also to provide charging mechanisms, so that the data assets can be monetized. In this respect, pricing models are needed to assign cost to data assets. An appealing starting point can be the Black-Sholes model [12] used for options pricing modeling. Along with the different possibilities of sharing data, it is also necessary to provide licensing levels and means for data providers to ensure that data assets are exploited under the negotiated conditions. The SynchroniCity architecture adopts as reference the specification of the business API ecosystem jointly provided by TM-Forum and the FIWARE initiative[3].

C. Security and access control

Closely related to data sharing provided by the marketplace, the platform needs to offer privacy and Authentication, Authentication and Accounting (AAA) mechanisms that enforce proper access to the data. In addition, from the data provider perspective, security needs to be also present between the underlying IoT urban infrastructure and the platform. This way, the injected data remain private until the data sharing policies are enforced by the platform. As for security, the architecture relies on the broadly adopted standard OAuth 2.0 [13]. This is the industry-standard for authorization, being defined by the IETF OAuth Working Group.

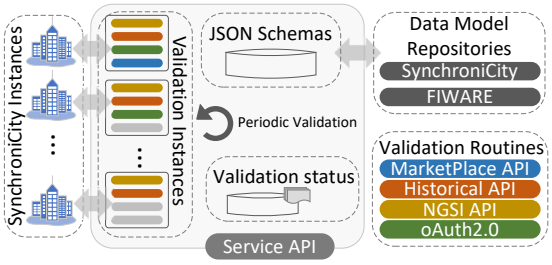

Fig. 1. Conceptual representation of the validation tool and flow

III. ASSESSING INTEROPERABILITY: METHODOLOGY AND VALIDATION TOOLS

As commented before, the proposed SynchroniCity architecture aims to ensure interoperability and service replicability. In this sense, it is of paramount importance to enforce that the interoperability points are compatible along multiple architecture instances. Having this in mind, a systematic validation methodology has been defined for the different functional requirements. This has permitted us to develop a validation framework[4], which ensures an interoperability certificate. Figure 1 depicts the validation cycle implemented by the tool. In short, the tool is configured with the same information required by service developers: endpoints and user credentials. Then, the validation framework starts a set of routines, each devoted to validate one specific interoperability requirement by performing a sequences of calls to ensure that the exposed APIs behave as expected. In addition, during the validation data assets are retrieved and analyzed to verify their compliance with the defined data-models. After the validation, compliance reports are created for each city, and they can be retrieved by using the API exposed by the framework[5].

In the following we will describe the functionalities implemented by the validation tool, which are tightly related to the interoperability requirements described in Section II.

A. Context information and historical data

The validation checks that a given end-point is able to perform the following actions:

- Context entity registration: allows registering and updating of registered context entities.
- Context entity search: allows the discovery and retrieval of the context entities.

[1]https://www.fiware.org/developers/data-models/
[2]https://gitlab.com/synchronicity-iot/synchronicity-data-models
[3]https://fiwaretmfbizecosystem.docs.apiary.io/

[4]The framework is publicly available in the SynchroniCity public repository: https://gitlab.com/synchronicity-iot/rz-instance-validator
[5]https://framework-validator.synchronicity-iot.smartsantander.eu/api-docs/

- Context entity update: allows updating context entities, related attributes and metadata. In addition, the endpoint must be able to perform the following updates:
  - *append*: add or update attributes in an existing entity, otherwise the entity is created with the given attributes.
  - *update*: update attributes in an existing entity.
  - *delete*: remove attributes from a specified entity. If no attribute is indicated, it will remove the entity context information.
- Context entity retrieval: gathering of context information related one or a list of entities.
- Context entity subscription: asynchronous notifications to context information, based on multiple criteria over context attributes.
- Data retrieval: gathering time series of a given attribute belonging to one entity. The API must allow pagination, and definition of temporal limits and order.

B. Data Models

The second validated feature is that related to the data representation. In this sense, the defined data models set syntactic and semantic requirements over the representation of urban data. Context entities are categorized according to the urban service they belong to, and classified by types (e.g. urban mobility service has entities of type BusStop). Data models are defined for each entity type, and the tool checks that all the entities 1) have the required attributes, 2) the attributes are properly formatted, and 3) the attribute value is meaningful (e.g. the temperature cannot be negative).

Since the number of entities can be very high, any lack of compliance when creating a type of entities would draw an intractable amount of error messages. In order to make the validation reports more usable, in case of data-model validation failure the report only contain a hint embracing detailed information of the first 5 context entities that are not compliant..

C. Security and access control

As mentioned before, OAuth 2.0 standard is adopted as the authorization solution within the implemented platform. In order to be compliant with most of existing tools, Synchronicity instances must implement the following authentication flows [13]:

- Authorization code grant: this is the most common flow. Using this flow the user grants clients a code to obtain an authorization code. It is typically used between public and private clients, such as a private server and a public web application.
- Implicit grant: it is similar to the previous case, but the token is granted instead of a code. It is typically used for public applications where the credentials cannot be securely stored.
- Resource owner password credentials grant: in this case the owner credentials are directly used as an authorization grant to obtain an access token. This authorization flow should only be used when there is a high degree of trust between the client and the owner of the resources.
- Client credential grant: this flow is used for clients to access resources about themselves, rather than those belonging to a user.
- Refresh token grant: eventually, this flow allows exchanging a refresh token when the access token has expired, so that clients continue having a valid access token without further user's intervention.

At the time of writing all the cities implementing the Synchronicity architecture have adopted widely used and trustfully OAuth 2.0 implementations.

D. Data Marketplace

Although the Data Market place may include several components (e.g. web portals), the interoperability validation focuses on the API. This allows data providers to register or import data, and publish offerings containing its description. In addition, the API also permits data consumers to discover and purchase data offerings.

Concretely, the following functionalities are validated:

- Data Source Specification: this permits defining data sources in the Market Place, from those accessible through the data APIs. In particular, a data source in the Market Place specifies how to access the data, and provides additional information such as a description, photos, etc. The validation tool ensures that it is possible to create, update, retrieve and list the specifications of data sources.
- Data Offering Management: this API permits the creation of data offerings on top of the specified data sources. It is worth noting that one offering may contain one or several data sources specifications. Similarly to the previous case, the validation checks that is possible to create, update, retrieve and list data offerings.
- Order Management: finally, the API also needs to provide offerings management. The actions over the offerings are the same as describe before: creation, update, retrieval and listing.

IV. SynchroniCity Santander Instance

For the time being, the SynchroniCity reference architecture has been deployed in 15 cities, and they expose above 400 thousands of data assets belonging to different city services [6].

In the following we describe the instantiation of the SynchroniCity architecture on top of the SmartSantander platform [14], following the layered approach depicted in Figure 2. In a nutshell, the IoT Management layer is responsible for the creation of data sets, whose access and management is supported by the Data management layer. The latter embraces

[6]The reader may refer to the following link to see the data assets exposed by each city and their validation status https://validation.services.synchronicity-iot.eu/table

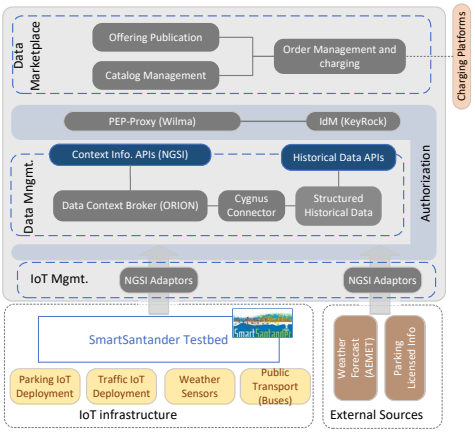

Fig. 2. Overarching SynchroniCity architecture

both context information and historical data APIs. On top of the Data Management functionalities, the data sharing and exploitation is governed by the Data Marketplace. Finally, the Authorization layer provides the required AAA functionalities along with privacy. In general, FIWARE [15] components have been adopted when possible, otherwise we implemented our own components compliant with the defined standards.

A. Components and interfaces for data management

As can be observed in Figure 2, the southbound architecture interacts with the IoT infrastructure and data sources through the IoT Management layer, so as to translate data into the defined data models. In the Santander instance, we have developed a set of NGSI adaptors able to interact with the SmartSantander APIs, as well as external sources. These adaptors have been developed using FIWARE IoT agents[7] as well as proprietary solutions when necessary. Most of the functionalities related to context data management are implemented by the ORION context broker. It implements the OMA-NGSI standards, and its most recent versions are starting to also implement ETSI NGSI-LD specifications. As shown in Figure 2, along with the context broker, the Data Management layer includes historical data storage enabled by the CYGNUS connector. Both context information entities and historical data are exposed through the corresponding interfaces.

B. Common data models

The data sets injected in the Data Management Layer follow the defined data-models and belong to the following urban services:

- Parking: real time information generated from buried parking sensors is available. In concrete, data assets include the status of more than 250 individual parking spots, as well as aggregated information of parking 23 areas in Santander downtown.
- Tourism: we have injected data of points of interest 2500 coming from different city services, as well as general city information. Under this category we include beaches, museums, libraries, or shops.
- Transportation: this category includes multi modal transport information from more than 450 traffic density sensors, 17 bike docking stations, and the public bus service. Concerning the latter, we have created data assets that represent bus lines, stops, and time arrival estimations to the different stops.
- Environmental monitoring : leveraging the SmartSantander infrastructure, data assets are created that provide real time information related to multiple environmental parameters. They include sound sensors, and mobile air quality sensors installed in buses, so moving all over the city.
- Weather information: apart from general environmental information, around 200 weather specific data assets are created using information from the large number of static sensors deployed in the city.
- Parks and gardens: the state of parks is also represented by 17 datasets which provide information about the air and soil.

As mentioned before, historical data of all the varying parameters of the aforementioned datasets is recorded and exposed through the historical data API, as shown in Figure 2.

C. Security

The security requirements are implemented based on the FIWARE generic enablers [15], providing security-related functionalities to the data consumption, communication with the IoT infrastructure and platform management. In particular the implementation relies on the KeyRock identity manager, that exposes the OAuth 2.0 interface, and the WILMA policy enforcement point which acts as a proxy for all the queries in the platform, thus ensuring that all the interactions pass through the authorization system.

In particular the following functionalities are implemented:

- Data protection and privacy
- Identity and authentication management
- Authorization and accounting
- Policy management

D. Data marketplace

Based on the previously presented functionalities the Data Marketplace permits the urban data consumption and monetization. This element is tightly integrated with the authorization framework, so to enforce correct control access and to modify it online according the transactions.

Using the Santander marketplace, data owners can create catalog of datasets and offers, as shown in Figure3. Then, registered users can get access to them either freely or purchasing them in accordance to the created offers.

[7]https://fiware-iot-stack.readthedocs.io/en/latest/device_gateway/#supported-protocols

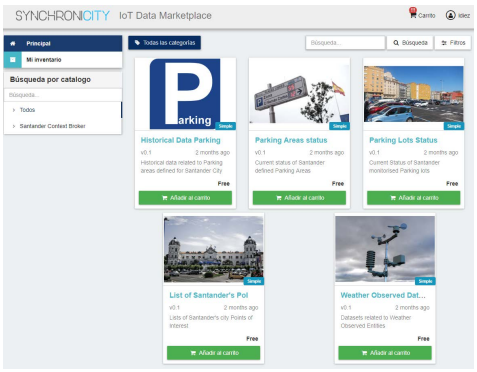

Fig. 3. Snapshot of the Santander data marketplace (https://marketplace.san.synchronicity-iot.eu)

V. Conclusion and Future Work

After more than one decade of the initial urban IoT massive deployments the requirements set up by city stakeholders, such majors, urbanists, activists or service providers, are well established. In parallel, technology has reached a maturity level which promises to fulfill most of the demands imposed by the urban ecosystem. However, it is not just a matter of technology maturity but guaranteeing that adopted solutions might easily be replicated reducing the corresponding investment expenses.

In this context, an open architecture which minimizes the number of interoperability points has been postulated. Its main pillars are the adoption of a common data model, a set of interfaces for managing both contextual an historical data, an access control and security framework. Last but not least, a data marketplace has been also integrated in this holistic architecture. In this respect, it is important to remark that being sustainability one of the main objectives (and potential stoppers) the ability to set up an agile and dynamic data market can become a key enabler in making such term a reality. Indeed, it seems quite evident that a data stock market is going to raise. In it the shares will be the different types of data which will evolve according to the relevance they might have depending on a plethora of considerations (imminent public procurement of the service or need to optimize services with high correlation with the one generating the relevant data).

Finally, it is also important to highlight the role that systematic validation tools will play when looking for replication and reusability. We have already presented the example of a tool which enables to assess the compliance of specific data models. The proliferation of such kind of tools should become a stimulus for easing the adoption of standards and its automatic validation.

Acknowledgment

This work has been partially funded by the European Union's Horizon 2020 Programme under Grant Agreement No. 732240 SynchroniCity (Delivering an IoT enabled Digital Single Market for Europe and Beyond). The content of this paper does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the authors.

In addition, this work has been also partially funded by the Spanish Government (MINECO) under Grant Agreement No. RTI2018-093475-AI00 FIERCE (Future Internet Enabled Resilient smart CitiEs)

References

[1] J. Exner, "The ESPRESSO - Project – A European Approach for Smart City Standards," in *Computational Science and Its Applications – ICCSA 2016*, 2016, pp. 483–490.

[2] "BIG IoT - Bridging the Interoperability Gap of the Internet of Things," http://big-iot.eu/, 2019-24-04.

[3] S. Soursos and I. P. Zarko, "symbIoTe: Symbiosis of Smart Objects Across IoT Environments," in *Digitising the Industry – Internet of Things Connecting the Physical, Digital and Virtual Worlds*, I. C. Book, Ed., 2016, pp. 303–307.

[4] M. Serrano, A. Gyrard, M. Boniface, P. Grace, N. Georgantas, R. Agarwal, P. Barnaghi, F. Carrez, B. Almeida, T. Teixeira, P. Cousin, F. L. Gall, M. Bauer, E. Kovacs, L. M. noz, L. Sánchez, J. Soldatos, N. Kefalakis, I. Abaitua, J. Echevarría, R. Steinke, M. Hauswirth, J. Kim, and J. Yun, "Cross-Domain Interoperability Using Federated Interoperable Semantic IoT/Cloud Testbeds and Applications: The FIESTA-IoT Approach," in *Building the Future Internet through FIRE: 2016 Fire book, a research and experimentation based approach*, 2017, pp. 287–321.

[5] "Itu-sg5, information and communication technologies for climate change adaptation in cities," http://www4.unfccc.int/nap/Documents/Supplements/ICTs-for-climate-change-adaptation.pdf, 2019-24-04.

[6] I. JTC1, "Smart cities. preliminary report 2014," https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/smart_cities_report-jtc1.pdf, 2019-24-04.

[7] AIOTI, "Aioti strategy 2017-2021," https://aioti.eu/wp-content/uploads/2017/11/AIOTI_Stategy_2017-2021_V1.0_FINAL_WEB.pdf, Tech. Rep., 2019-24-04.

[8] "Itu-sg20, focus group on data processing and management to support iot and smart cities & communities," https://www.itu.int/en/ITU-T/focusgroups/dpm/Pages/default.aspx, 2019-24-04.

[9] U4SSC, "United for smart sustainable cities – overview," https://www.unece.org/fileadmin/DAM/hlm/projects/SMART_CITIES/U4SSC-brochure.pdf, Tech. Rep., 2019-24-04.

[10] "Oma, ngsi context management," http://www.openmobilealliance.org/release/NGSI/V1_0-20120529-A/OMA-TS-NGSI_Context_Management-V1_0-20120529-A.pdf, Tech. Rep., 2019-24-04.

[11] "ETSI-CIM, Draft ETSI GS CIM 004 V0.0.11 (2018-02). Context Information Management (CIM); Application Programming Interface (API)," https://www.etsi.org/deliver/etsi_gs/CIM/001_099/004/01.01.01_60/gs_CIM004v010101p.pdf, Tech. Rep., 2019-24-04.

[12] F. Black and M. Scholes, "The pricing of options and corporate liabilities," *Journal of Political Economy*, vol. 81, no. 3, pp. 637–54, 1973. [Online]. Available: https://EconPapers.repec.org/RePEc:ucp:jpolec:v:81:y:1973:i:3:p:637-54

[13] D. Hardt, "The OAuth 2.0 Authorization Framework," Internet Requests for Comments, RFC Editor, RFC 6749, October 2012, http://www.rfc-editor.org/rfc/rfc6749.txt. [Online]. Available: http://www.rfc-editor.org/rfc/rfc6749.txt

[14] L. Sánchez, V. Gutiérrez, J. A. Galache, P. Sotres, J. R. Santana, J. Casanueva, and L. Muñoz, "Smartsantander: Experimentation and service provision in the smart city," in *2013 16th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, June 2013, pp. 1–6.

[15] "FIWARE programme," https://www.fiware.org/, 2019-24-04.