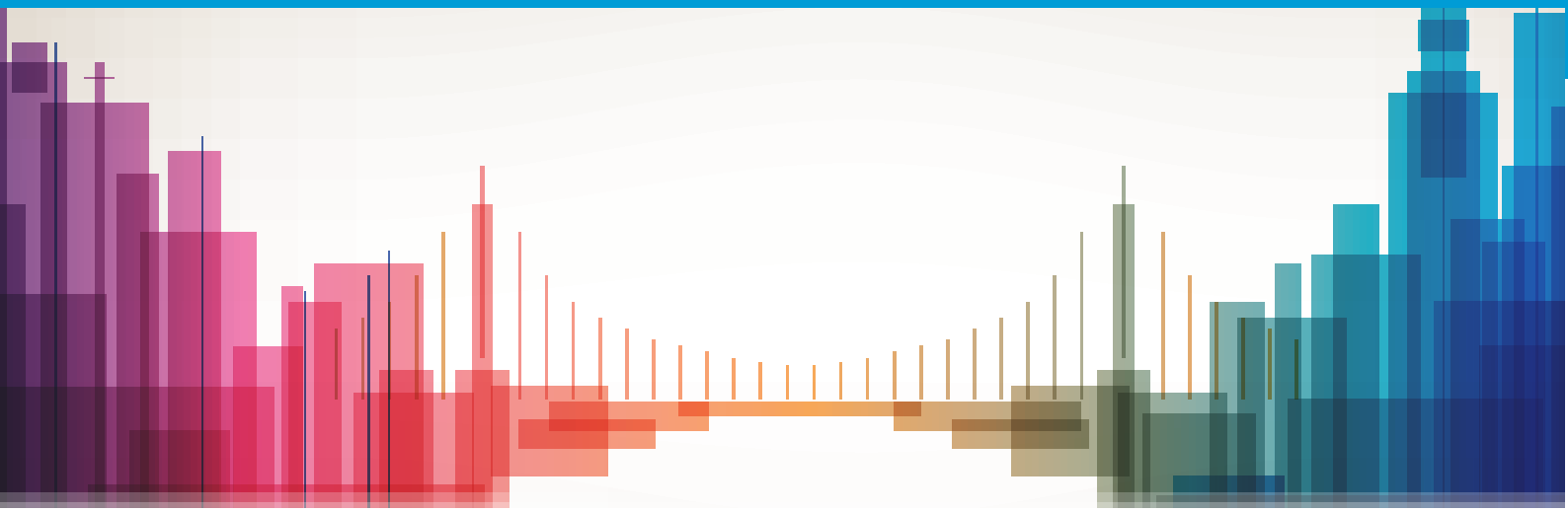
Data and API requirements for decentralized smart city platforms



Convention on Biological Diversity

United Nations ECLAC

Food and Agriculture Organization of the United Nations

UNIDO

ITU

UNDP

United Nations Economic Commission for Africa

UNECE

UNESCO United Nations Educational, Scientific and Cultural Organization

UN environment programme

UNEP FINANCE INITIATIVE

United Nations Framework Convention on Climate Change

unitar United Nations Institute for Training and Research

UN HABITAT FOR A BETTER URBAN FUTURE

United Nations Department of Economic and Social Affairs

UN OFFICE 4 PARTNERSHIPS

UNU EGOV

UN Tourism

UN WOMEN

WORLD METEOROLOGICAL ORGANIZATION

Data and API requirements for decentralized smart city platforms

Foreword

This publication was developed within the framework of the United for Smart Sustainable Cities (U4SSC) initiative.

Acknowledgments

The development of this deliverable was led and coordinated by Leonidas Anthopoulos, Greece.

This publication was authored by Leonidas Anthopoulos from Greece.

The author would like to thank the following contributing individuals: Ioannis Nikolaou (PhD, University of Thessaly, Greece) and Christos Ziozias (PhD, University of Thessaly, Greece).

The author would also like to thank the following experts for their valuable comments and discussion: Felix Villanueva (Universidad de Castilla-La Mancha), Adam Obeid (Ogero Telecom, Lebanon), Asma Karoui (GIZ, Tunisia), Jeronimo Hinojosa (Valladolid City Council, Spain), Klaus Hoeckner (Hilfsgemeinschaft der Blinden und Sehsch, Austria), Xiongwei Jia (China Unicom, China) and Straton Ndikuryayo (Independent Consultant).

The author wishes to thank the U4SSC management team: Okan Geray (U4SSC Chair), Ramy Ahmed Fathy, Giampiero Bambagioni, Paolo Gemma, Wendy Teresa Goico Campagna, Tania Marcos and Emily Royall (U4SSC Vice-Chairs) for their assistance and contributions.

The author also extend their gratitude to the contributing organizations, along with their representatives: Oliver Hillel from the Convention on Biological Diversity (CBD), Lucy Winchester and Vera Kiss from the Economic Commission for Latin America and the Caribbean (ECLAC), Simone Borelli from the Food and Agriculture Organization (FAO), Cristina Bueti from the International Telecommunication Union (ITU), Deniz Susar from United Nations Department of Economic and Social Affairs (UNDESA), Iryna Usava from the United Nations Development Programme (UNDP), James Murombedzi from the United Nations Economic Commission for Africa (UNECA), Tea Aulavuo and Maike Salize from the United Nations Economic Commission for Europe (UNECE), Guilherme Canela from the Regional Bureau for Sciences in Latin America and the Caribbean of the United Nations Educational, Scientific and Cultural Organization (UNESCO), Gulnara Roll from United Nations Environment Programme (UNEP), Matthew Ulterino from the United Nations Environment Programme Finance Initiative (UNEP-FI), Motsomi Maletjane from the United Nations Framework Convention for Climate Change (UNFCCC), Edlam Abera Yemeru and Roberta Maio from the United Nations Human Settlements Programme (UN-Habitat), Katarina Barunica Spoljaric and Nicholas Dehod from the United Nations Industrial Development Organization (UNIDO), Ebru Canan-Sokullu from United Nations Institute for Training and Research (UNITAR), William Kennedy from the United Nations Office for Partnerships (UNOP), Soumaya Ben Dhaou from the United Nations University – Operating Unit on Policy-Driven Electronic Governance (UNU-EGOV), Sylvia Hordosch from the United Nations Entity for Gender Equality and the Empowerment of Women

(UN-Women), World Meteorological Organization (WMO) and Sandra Carvao from the World Tourism Organization (UN Tourism).

Disclaimer

The opinions expressed in this publication are those of the authors and do not necessarily represent the views of their respective organizations or U4SSC members. In line with the U4SSC principles, this report does not promote the adoption and use of any specific digital transformation technology. It advocates for policies encouraging responsible use of information and communications technologies (ICTs) that contribute to the economic, environmental and social sustainability as well as the advancement of the 2030 Agenda for Sustainable Development and the Pact for the Future and its Global Digital Compact.

ISBN

978-92-61-40361-4

Contents

List of figures

Figures

Abbreviations and acronyms

Abbreviation	Full Form
AI	Artificial Intelligence
API	Application Programming Interface
ABAC	Attribute Based Access Control
ACL	Access Control Lists
DCITY	Decentralized Smart City environment
DID	Decentralized Identifiers
DLT	Distributed Ledger Technology
HLA	High-Level Architecture
ID	Identifier
IDS	International Data Spaces
IoT	Internet of Things
ML	Machine Learning
RBAC	Role-Based Access Control
SC	Smart City
SCHub	Smart City Hub
SCP	Smart City Platforms
VC	Verifiable Credentials

Executive summary

This document introduces a decentralized approach to the smart city data management that is labeled decentralized smart city environment and enables the users to have full control over their data. This decentralized approach can apply rules on data ownership, while it is expected to enable the development of new social value through increased transparency and equity in data access, and even enable the appearance of new business models.

The report presents the existing standards for data privacy during data flows in smart city. Moreover, the decentralized smart city environment reference architecture is introduced and explained, it will be scalable, open and privacy aware. Additionally, when decentralized smart city environment will be clarified in technological terms, it can show how it can be "adjusted" to serve any type of city, and the standardization of its flows can be defined.

In this respect, the contribution of this report is twofold: i) it justifies and determines how the management of the access control to a set of data by the data owners and the selective access to subsets of the data for different users and different services can be achieved, and ii) provides the reference architecture of decentralized smart city environment.

1 Introduction

This document deals with the following problem: The Smart City (SC) is evolving to a Hub, which brings together all the city data and resources, to achieve the goals and fulfill the purposes that it has set itself effectively and seamlessly. The ownership of these data and the ways in which it is collected, shared, processed and transformed into information, is still under investigation. Moreover, the collected data can contain personally identifiable information, and may be subject to privacy and data protection regulations, including the "right to be forgotten". Even if the data are anonymized to remove the sensitive information, the use of the metadata in conjunction with artificial intelligence / machine learning (AI/ML) algorithms can still produce information that can be of a sensitive nature.

The access to the Smart City data is not standardized and is primarily platform specific as there is limited research that focuses on corresponding standardization. The data storage options vary from data dumps in files to access through application programming interfaces (APIs) for more advanced platforms. In all cases, the Smart City platform administrators have full access to the data. It is also very hard, and in some cases even impossible, to control which subset of the data will be accessible to third-party platforms and services. Once access is granted it is not practically possible to apply a fine-grained Role-Based Access Control (RBAC) on the data itself. Usually, RBAC is applied on the type or the location of the data sources.

The existing centralized approach has the following drawbacks:

- No requirements for the API standardization are introduced to the data providers.
- When the central authority is compromised by internal or external attackers, they gain access to the complete set of the data.
- The users, who are the producers of the data, have no control over how their data are used and shared.

This initiative aims to introduce a decentralized approach to the Smart City data management so enabling the users to have full control over their data. This decentralized approach will apply rules on data ownership, while it is expected to enable the development of new social value through increased transparency and equity in data access, and even enable the appearance of new business models.

This document aims to provide answers to the following research questions:

1) How can the Smart City platform be transformed into a decentralized environment (DCITY) that will ensure data privacy and data ownership?
2) What are the requirements and the architecture of the decentralized smart city environment ?

Initially the appropriate standards for data privacy during data flows in Smart City must be defined (RQ1). Moreover, this decentralized smart city environment standardization and interoperability

must be secured to allow the management of the access control to a set of data by the data owners and the selective access to subsets of the data for different users and different services. Finally, the decentralized smart city environment reference architecture must be determined (RQ2). These efforts will help the cities and communities to host "a decentralized system - the decentralized smart city environment", which will be scalable, open and privacy aware. Additionally, when this environment is clarified in technological terms, it will show how it can be "adjusted" to serve any type of city and the standardization of its flows can be defined. As such, the contribution of this study is twofold: i) it determines how the management of the access control to a set of data by the data owners and the selective access to subsets of the data for different users and different services can be achieved; and ii) it provides the reference architecture of a decentralized approach.

2 Background

Although "city hubness" has been discussed broadly in urban studies, the smart city decentralization is still missing from the literature. Furthermore, the smart city appears to concern "innovation" in the urban space based primarily on information technologies; however, this innovation role is still under exploration. Big vendors view the Smart City as an open platform that boosts city innovation and must be explored further for this innovation potential.

Several smart city platform installations exist around the world. Some cities use open platforms, while others have installed commercial products that also serve the demand for city's data collection, analysis and visualization, and for remote utility management, which concern the traditional Smart City-as-Hub approach [1]. The wealth of data produced by the smart city sensors can be used either as they are or combined with one another to provide additional insights using data fusion techniques [17]. Decentralized smart city environments have not yet appeared, regardless the existence of decentralized solutions used in cities (e.g., tokenization, decentralized autonomous organizations,). Moreover, data privacy and ownership have not yet been standardized in smart city environments and the corresponding research is missing, regardless the corresponding policy-making efforts that can be observed (i.e., from the European Commission [18]).

3 Gap Analysis on data sovereignty

The need for data sovereignty among the wealth of available data providers, on cloud and on premises, has led to the appearance of various initiatives. Among the most active ones in the European Union are International Data Spaces (IDS) and Gaia-X [19].

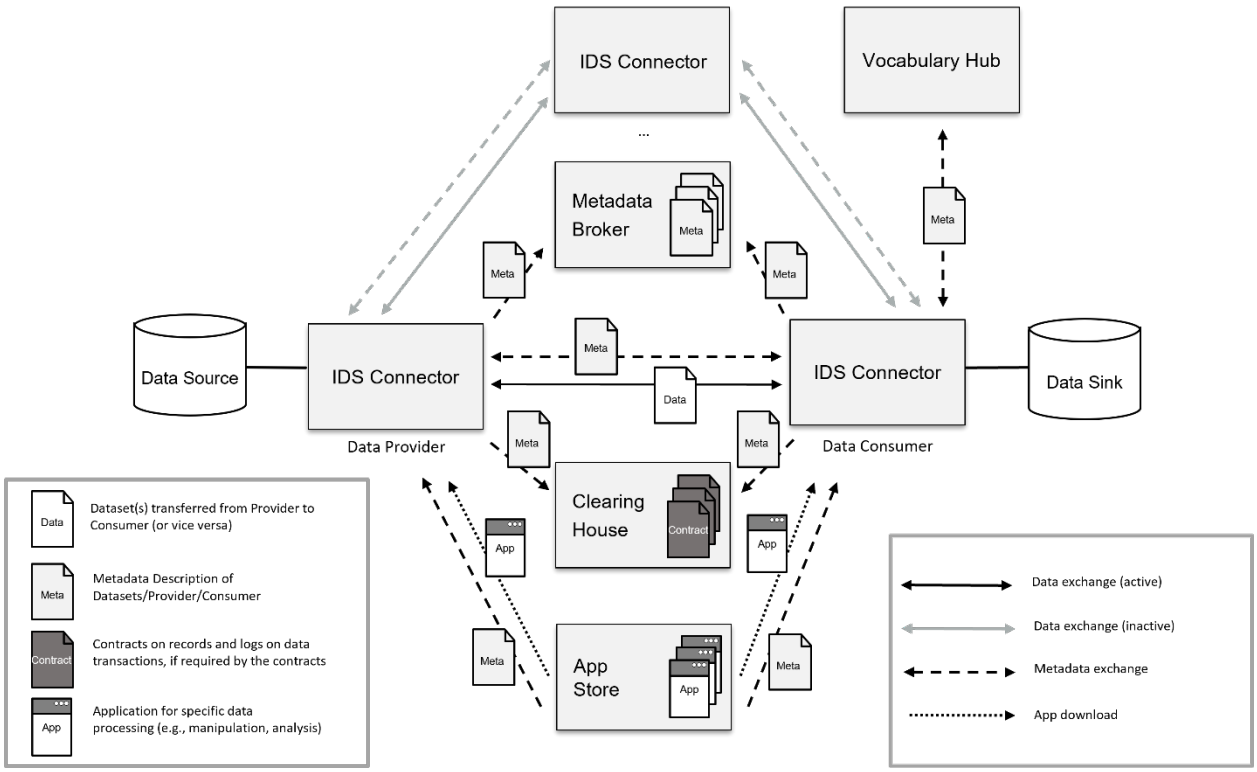
3.1 International data spaces: strategies and choices

Data spaces is an initiative to enable the seamless exchange of information among independent data providers in a secure, self-sovereign and standardized way. As described in the purpose statement of data spaces [13]:

"The international data spaces (IDS) are virtual data spaces leveraging existing standards and technologies, as well as governance models well-accepted in the data economy, to facilitate secure and standardized data exchange and data linkage in a trusted business ecosystem. It thereby provides a basis for creating smart-service scenarios and facilitating innovative cross-company business processes, while at the same time guaranteeing data sovereignty for data owners."

A reference architecture has been proposed that provides guidance on the implementation of such a data space in accordance with the initiative's goals and values. The reference architecture is defined in the business, functional, information, process and system layer; the latter is depicted in the figure below (Figure 1).

Figure 1: IDS System Layer (Source: IDS RAM, 2023)



International data space focuses on the process, governance and data exchange among the various participants and is agnostic on the underlying infrastructure. However, as this is equally important for the overall data management strategy, a separate initiative has been looking into this, namely Gaia-X.

3.2 Gaia-X

Gaia-X is an initiative to develop a federated secure data infrastructure based on the values of transparency, openness, data protection and security, which can be applied to cloud technologies to obtain transparency and controllability across data and services (Figure 2). As described in the Vision & Strategy document [14]:

"Gaia-X represents the next generation of data infrastructure: an open, transparent, and secure digital ecosystem, where data and services are available, collated, and shared in an environment of trust.

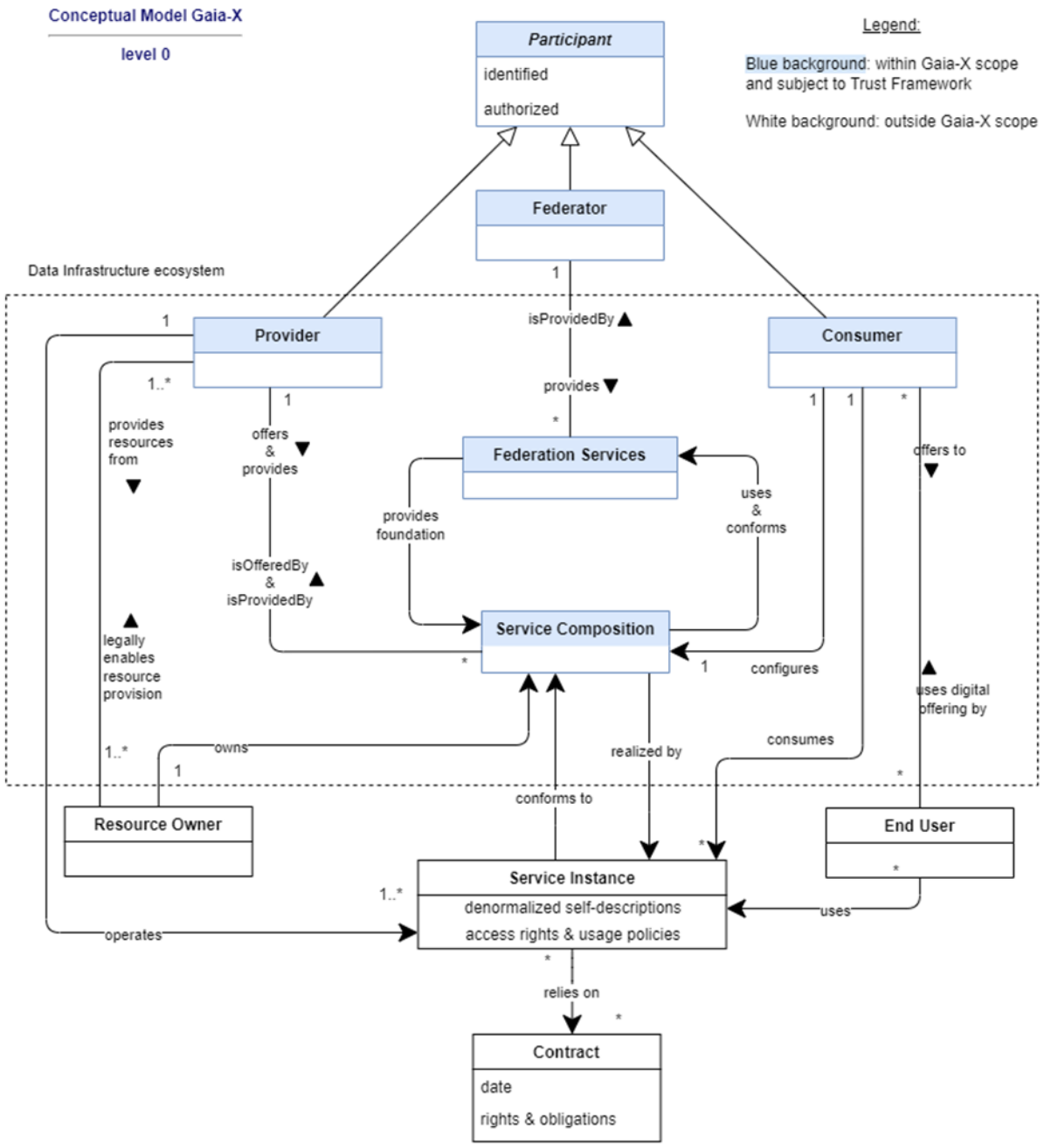
The architecture of Gaia-X is based on the principles of decentralisation and federation. Gaia-X allows many individual platforms to follow a common standard – the Gaia-X standard to work together."

The goals of Gaia-X are to:

- Define Gaia-X architecture & rules
- Provide open implementation
- Act as a qualification authority for Gaia-X compliance

Although not specific to Smart Cities, or Smart City Platforms (SCPs), Gaia-X can provide guidelines for allowing the interoperability between SCPs of SCPs and other platforms, as long as all involved parties a Gaia-X compliant.

Figure 2: Gaia-X conceptual model (Source: Gaia-X Architecture Document - 22.10 Release, 2023)



4 Data sovereignty and API requirements in a Decentralized Smart City

Applying the decentralized model in the smart city context introduces a whole new range of possibilities for the lifecycle of IoT devices and data management, from the roll out, to operations and decommissioning of the devices. Our focus in this document is data sovereignty, privacy and ownership. The traditional centralized approach (described as Smart City-as-Hub architecture [1]) of

a smart city assumes the responsibility for generating, transmitting, and storing the data produced by the Internet of Things (IoT) devices is delegated from the smart city Authorities to the IoT platform vendor. A decentralized model of a smart city, the decentralized smart city environment, does not make any assumption or delegation of responsibility among the various actors but rather allows them to explicitly and autonomously decide how the data are transmitted, stored and shared.

A comparison of the current centralized model with the envisioned decentralized approach is presented in the following sections.

4.1 Centralized approach

The centralized model in data ownership is best presented in the form of an example. A smart city uses smart water-meters in order to monitor and manage water consumption. The devices generate a time-series of measurements for each water meter that belongs to a specific household. These data may be of interest to stakeholders that should have access to a subset of this data: they could have access to the consumption pattern without knowing to whom the data belong, or have access to the owner and the monthly data of some users but not others.

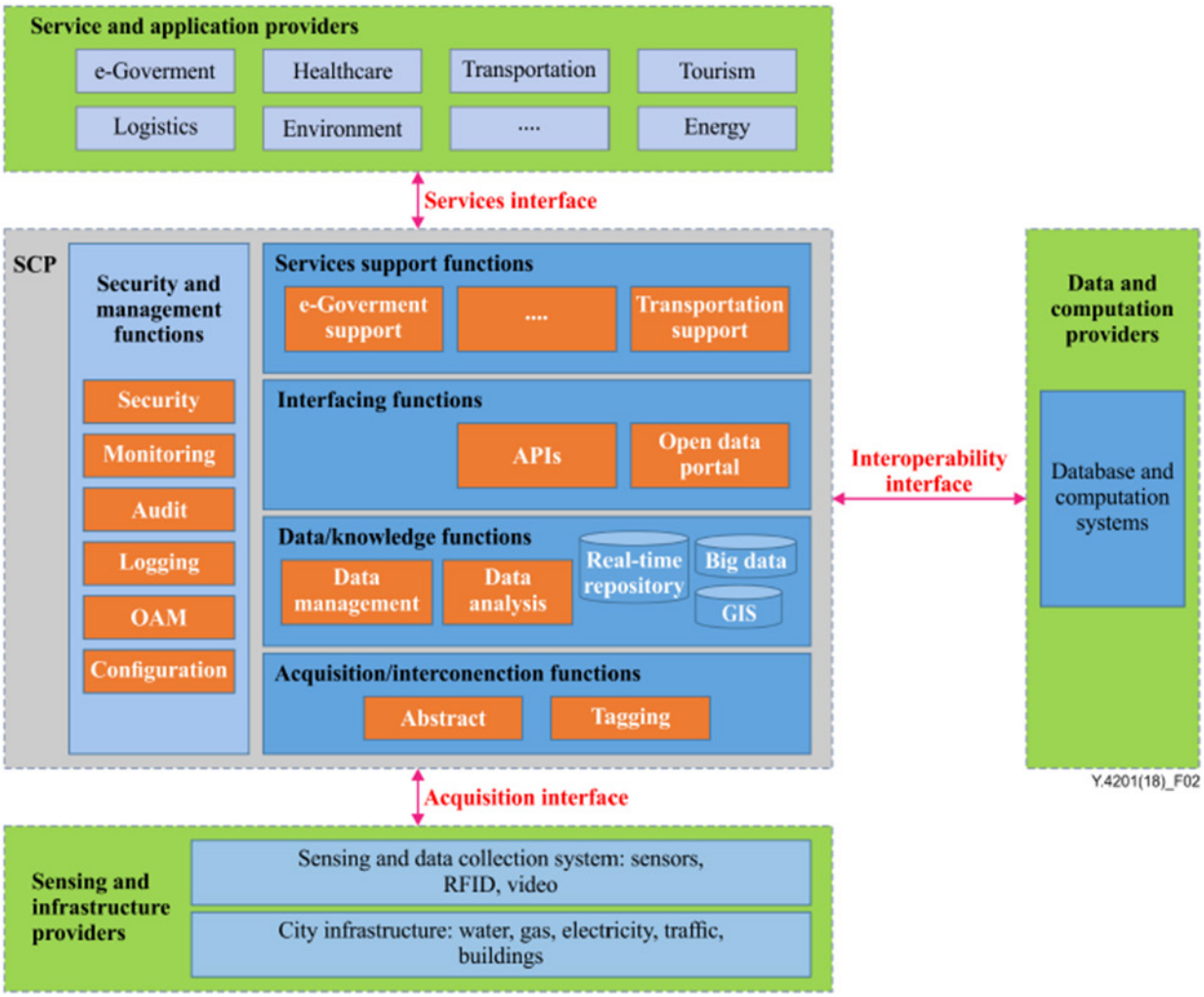
The traditional approach to solving this problem is to have data stored in a centralized database owned by an authority that has complete access to all information. This authority allows selective access to this data to external services using RBAC, Attribute Based Access Control (ABAC), Access Control Lists (ACL) or similar pattern.

The centralized nature of this approach has the following drawbacks:

- the central authority can be compromised by internal or external attackers who can gain access to the complete set of the data; and
- the producers of the data have no control over how their data are used and shared

The Reference framework of an SCP (ITU-T Y.4201) [16] in Figure 3 depicts this scenario in detail when assuming that the "Database and computation systems" on the right are centralized databases.

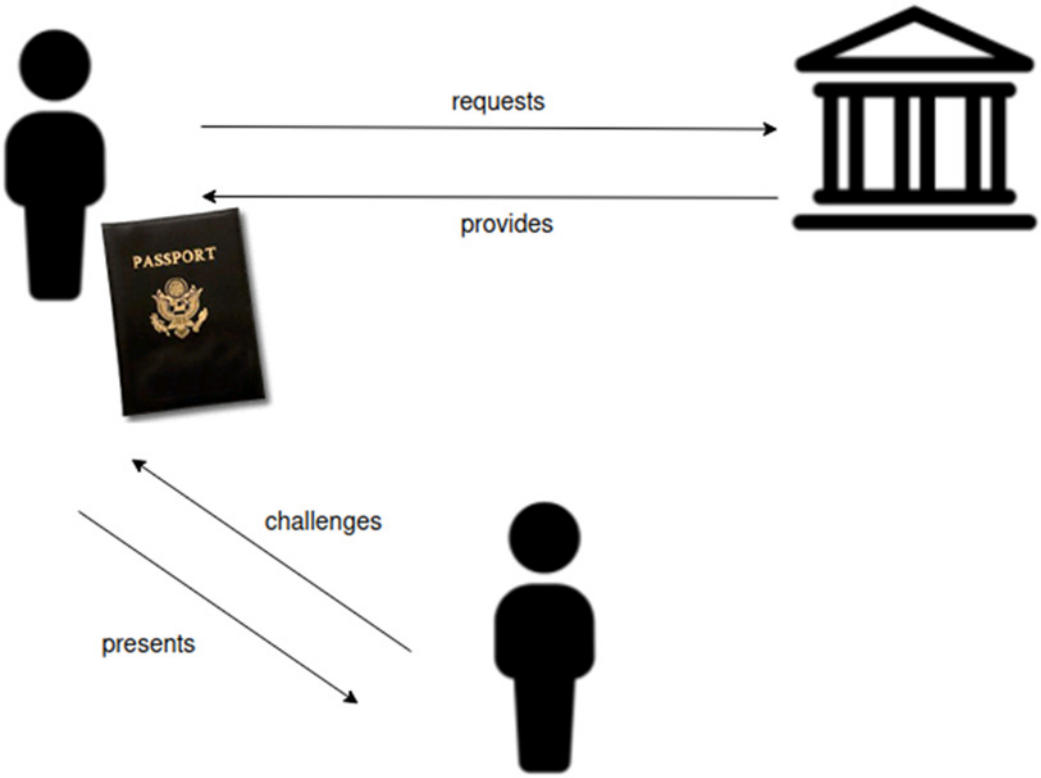
Figure 3: Reference framework of an SCP (Source: Recommendation ITU-T Y.4201)



4.2 Decentralized approach

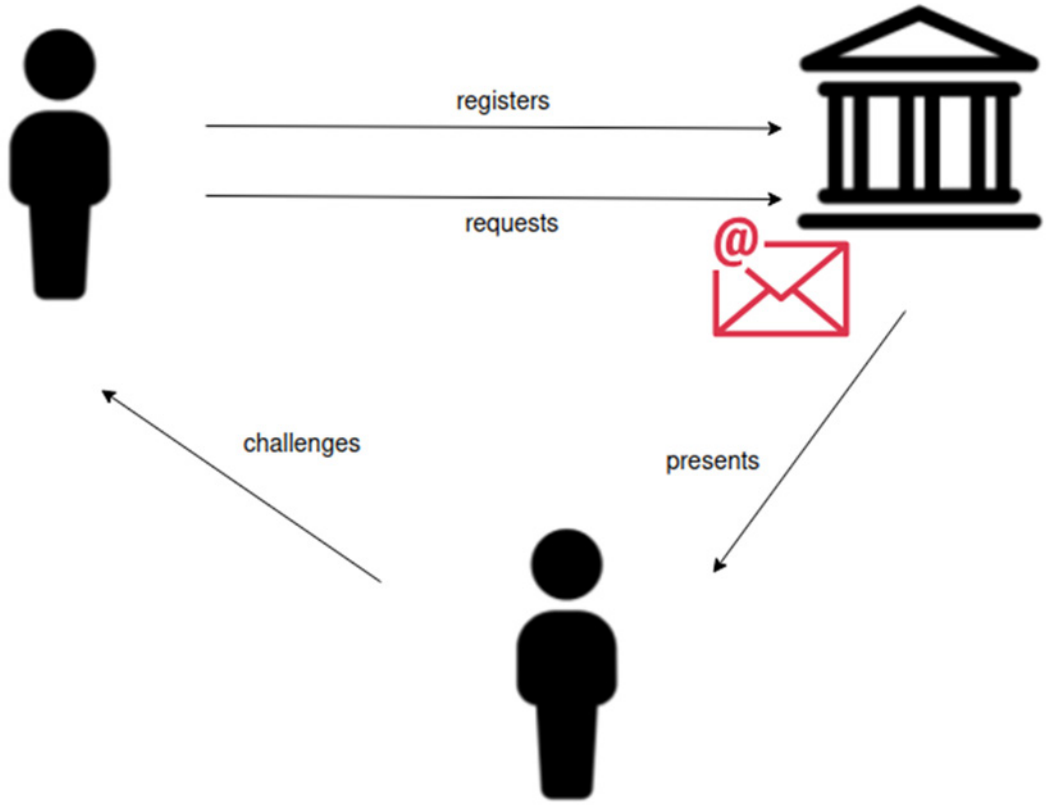
In the "analogue" world, the identity and data management are mostly decentralized. Taking the proof of identity using a passport as an example, the passport document is issued by an issuing authority and handed physically to the owner. When the passport holders want to prove their identity to another authority, e.g., the immigration control in an airport, they physically present the passport document. Assuming the immigration control trusts the issuing authority, access is granted to the individual. In this simple example the proof of identity was always at the hands of the individual, and the passport holder was in control of when, how and to whom they presented it.

Figure 4: Analogues approach to identity issuing, validation and verification (Source: Author)



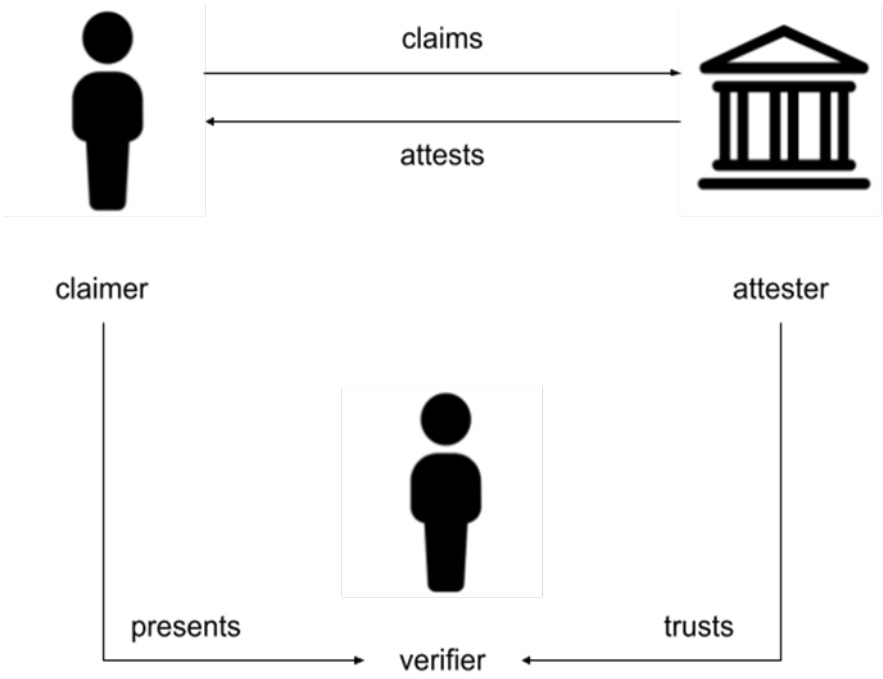
In the virtual world, proof of identity is controlled centrally by the issuing authorities and can be modified, shared or even deleted without any control by the individual. As an example, a simplified identity flow looks something like this: a user requests an identity account (e.g., an e-mail) from a provider. Using this e-mail, the user registers on an online service. The service is using the provided identity to validate the user's identity via, for example, a verification e-mail or a single-sign-on token. After successful registration, the user can use this identity to access the service. The identity itself, however (i.e., the e-mail account) is not physically owned by the user. In fact, the identity provider can disable access to the account thus restricting or even completely disabling the user's access to the service.

Figure 5: Digital, centralized approach to identity issuing, validation and verification (Source: Author)



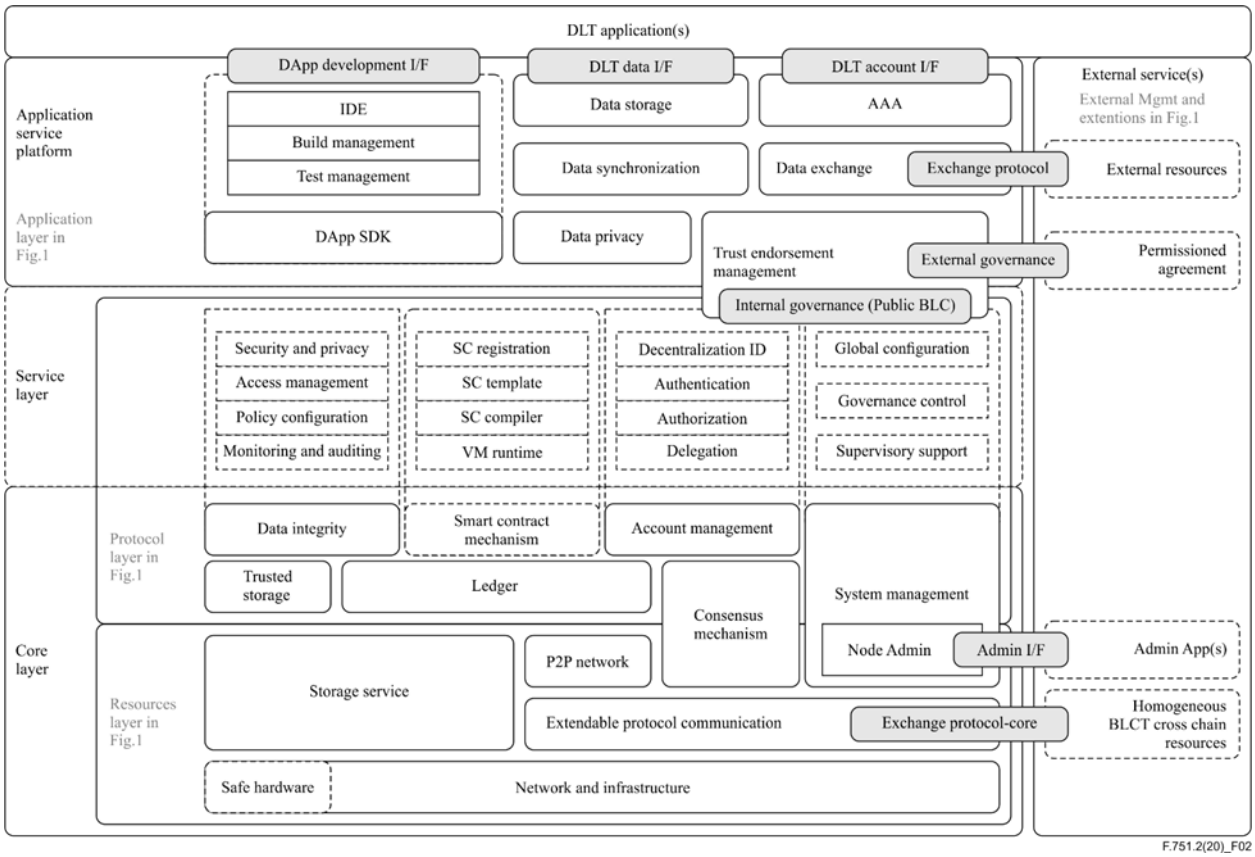
The Decentralized Identifiers (DID) [3] and Verifiable Credentials (VC) [8] provide a decentralized approach to identity issuing, validation and verification. Instead of a centralized authority that issues, owns and manages the identity information of an entity, the entity itself is issuing "claims" that are "attested" by authorities. For example, an individual creates a "claim" that she is 18 years old, has a permanent address and that she can drive a car. This claim is presented to one or more authorities that "attest" them, e.g., a municipality that, after confirming the person's date of birth and residence, confirms the respective claims and a driving examination centre that confirms that the person has successfully completed the driving lessons and practical examination. Once the claim is attested by these two authorities, the person can present it to anyone who requests this information. The claim itself is owned and controlled by the person, not the attestation authorities. When someone requests the person to prove the claim, the person presents it, and the verifier confirms that: a) the attestation authorities are trusted; b) that the attestation has not been revoked; and c) that the claim is valid. If not, all information needs to be disclosed to the verifier, for example when the individual is requested to present their driver's licence to a police officer, they can choose to disclose their age and driving ability but not their address. This selective disclosure of identity information is, in fact, a step further to the "analogue" identity management (Figure 6).

Figure 6: Digital, decentralized approach to identity issuing, validation and verification (Source: Author)



A decentralized approach to the identity management utilizing DID and VC would allow users to have control over their identity [3, 6] and data. This decentralized approach will apply rules on data ownership [5, 7], while it is expected to enable the development of new value and corresponding business models [4, 9]. The use of VC as a means to achieve decentralization is also included in the Gaia-X Trust architecture and trust framework [11, 12]. In addition, as a starting point of the decentralized smart city environment architecture the latest architectural approaches (i.e., based on ITU T Recommendation ITU-T F.751.112 [10]) (Figure 7) can be used.

Figure 7: Schematic diagram of the detailed Distributed Ledger Technology (DLT) architecture (Source: Recommendation ITU-T F.751.2)



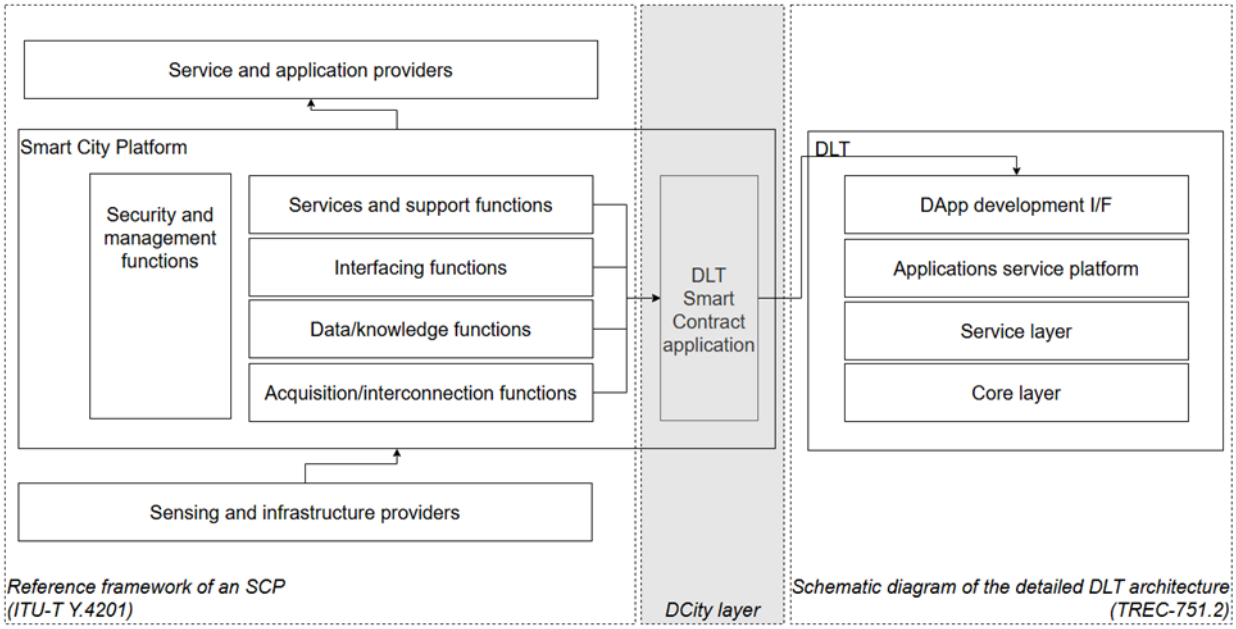
Another aspect of the smart city that can move from centralized to decentralized architectures is that of Software-as-a-Service (SaaS) applications. In traditional deployment models, a web application that accesses a service to retrieve data relies on executable code that is developed, deployed, and operated by specific companies or organizations. The developers, operators and administrators of these companies have complete control over the execution environment of the code that provides each service. For this reason, security policies and controls are put in place so that any abuse of this power has legal repercussions.

The decentralized equivalent of centralized owned and operated executable code is a Smart Contract [7, 9]. A Smart Contract in simple words is a computer program that is deployed in such a way that when executed no one, including the author of the code itself, has control over its state and execution environment and cannot modify it without being detected. In other words, a Smart Contract is a computer program that is autonomous. The Smart Contract introduces a completely new domain for application that can operate in a completely trustless environment without the need for a central authority.

4.3 High Level Architecture of decentralized smart city environment

The High-Level Architecture (HLA) of decentralized smart city environment combines the HLAs of the Smart City with the HLA of Distributed Ledger Technology (DLT) architecture in order to enable the use of verifiable credentials (VC) in the smart city context. The integration point of the two architectures is the Data and Computation providers' part of Figure 3 and the DLT Application layer of Figure 7. The Reference Architecture of the decentralized smart city environment is depicted in Figure 8.

Figure 8: Decentralized smart city environment reference architecture (Source: Author)

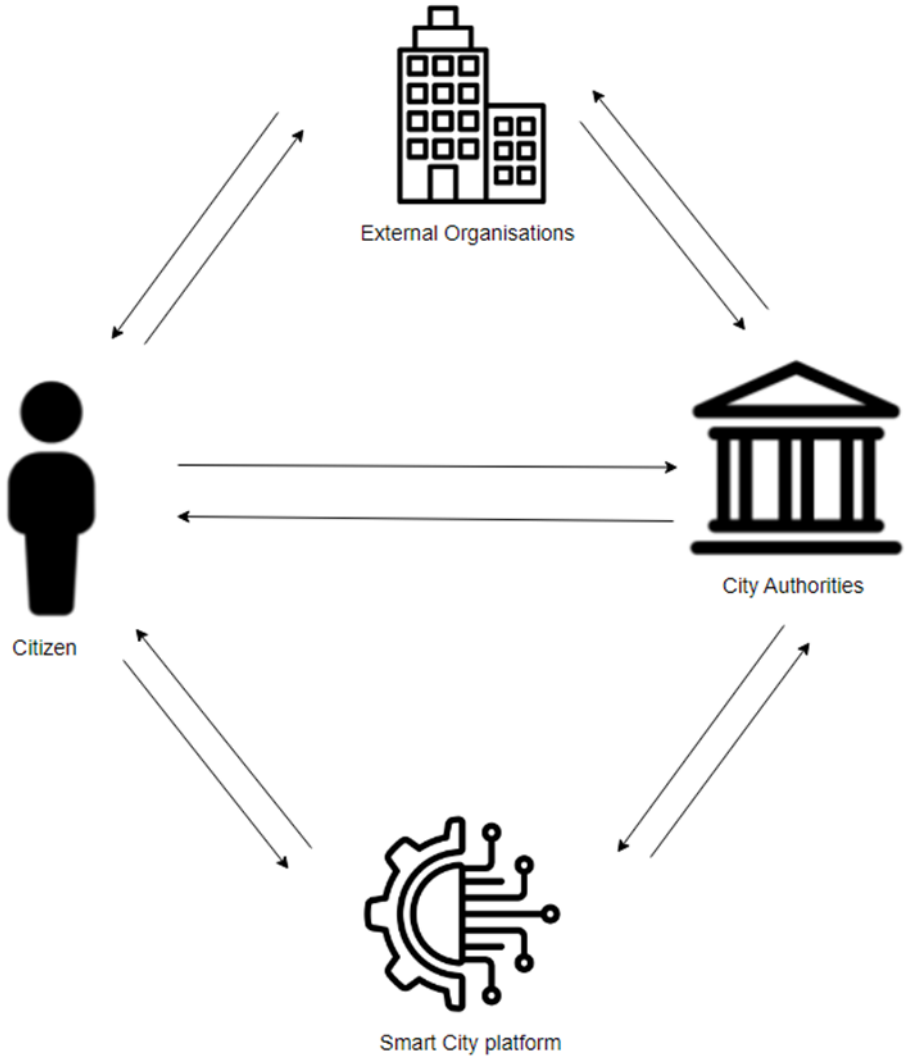


The left part of the reference architecture is described in detail Reference framework of an SCP Recommendation ITU-T Y.4201 [16], whereas the right part is discussed in detail in Recommendation ITU-T F.751.2: Reference framework for distributed ledger technologies [10]. The decentralized smart city environment layer is depicted in between and is where the VC are implemented as a set of Smart Contracts in a DLT application that runs on top of a DLT. This will enable the smart city infrastructure to leverage them in the data management flows. This integration will make possible data flows that allow a Smart City citizen to control the access to the data that are generated by IoT devices in a decentralized and self-sovereign fashion.

In the scenario depicted in Figure 9, the City Authorities provide the attestation services to all smart city platform stakeholders. The citizens, smart city platform providers and external organizations obtain VC that include their claims on what data they can provide or have access to. Subsequently, in each interaction among these parties, every request is validated against these claims. The decentralized nature of this approach does not require the validation of each request with the involved parties. As long as a stakeholder trusts the cryptographic signature of the rest, then it

is sufficient to validate the claims presented and, if they are cryptographically correct, fulfill the request.

Figure 9: Decentralized smart city environment stakeholder interactions (Source: Author)



As an example, we can consider citizens who have a smart water meter with a unique identifier (ID) installed in their property. The citizens obtain an attestation from the city authorities for a claim that a meter with the said ID is installed in their property. An external organization responsible for billing obtains an attestation for the city authorities to access the measurement data of smart water meter devices only. The smart city platform provider trusts the attestation issued by the city authorities. With this setup, citizens can request access to their data from the smart city provider by presenting the claim that they own the smart meter without disclosing any other additional information about their identity. The smart city platform provider can validate the claim is valid and provide the requested data. At the same time, the external organization responsible for the billing

can request the measurement information for all water meter using their claim that the smart city provider can also validate without obtaining any additional information about the citizens data.

4.4 A note on DLT energy consumption

The selection of the DLT technology can have an enormous impact on its energy consumption. The various DLT models have been analysed in detail in [15]. The summary of the relationship between energy consumption and DLT usage is that as the level of trust among the participants decreases, the energy consumption increases. For smart city applications it is assumed that the stakeholders are participating in good faith and have agreed on the common goal of service the citizens need in the best possible way. For this reason, it is recommended to deploy a DLT infrastructure that uses either Proof of Stake (PoS) of Proof of Authority (PoA) consensus models, which have significantly less energy consumption compared with the Proof of Work (PoW) that is used in the cases in which the DLT participants cannot assume any level of trust among them.

4.5 Decentralized smart city environment requirements

In the previous sections, we have assumed the existence of a Smart City Platform and a DLT for supporting the decentralized smart city environment architecture. These are the minimum requirements for the decentralized smart city environment concept as they fulfill the following roles:

1) The Smart City Platform provides all the functionality described in Recommendation ITU-T Y.4201 [16] in order to support the smart city functions. This functionality could be implemented as Smart Contracts running on-chain on the DLT. However, the code complexity of this approach would be significantly higher. Furthermore, the performance of Smart Contracts execution is order of magnitudes lower than that of the code used by the Smart City Platform. It is, therefore, not practically possible to replace the Smart City Platform with a DLT.
2) The DLT provides the decentralization aspect of the decentralized smart city environment concept. This cannot be implemented using the standard software architectures used in a Smart City Platform. Consequently, it is mandatory to deploy a DLT as part of the decentralized smart city environment architecture. The only requirement for the DLT itself is the support of Smart Contracts that can be used to implement the VC and DID that have been discussed in the previous sections.

5 Conclusions

Decentralized smart city environment is an innovative approach, with significant areas for study and development, and with high potential impact, since it addresses forthcoming urban challenges and views the dynamic smart city domain from a highly systemic and social perspective, including the existing privacy concerns [20].

In terms of the research questions introduced in this document, the use of VC and/or other decentralized technologies for identity and data management can advance smart city platforms to a decentralized smart city environment model (RQ1). The architecture of the decentralized smart city environment will expand on the existing SCP and DLT architectures and provide the connection among the components needed to achieve decentralization (RQ2).

A decentralized approach in the data management of the smart city data can have far fetching implication in other areas as well, as for example that of data fusion. The introduction of data ownership and control mechanism for the data producer may disrupt the current approaches used to combine data from various data sources. At the same time, these mechanisms can lead to higher engagement of the smart city citizen who will have to be at least informed and possibly actively involved in initiatives that make use of their data.

References

[1] Anthopoulos, L. G., Pourzolfaghar, Z., Lemmer, K., Siebenlist, T., Niehaves, B., & Nikolaou, I. (2022). Smart cities as hubs: Connect, collect and control city flows. Cities, 125, 103660. https://doi.org/10.1016/j.cities.2022.103660

[2] Cruz, J. P., Kaji, Y., & Yanai, N. (2018). RBAC-SC: Role-Based Access Control Using Smart Contract. IEEE Access, 6, 12240-12251. https://doi.org/10.1109/access.2018.2812844

[3] Decentralized Identifiers (DIDs) v1.0. (2022). Accessed, July 2022 at www.w3.org website: https://www.w3.org/TR/did-core/

[4] Gillai, B., & Mendelson, H. (2020, November). Creating Value with Blockchain: A Value Chain Management Perspective. Retrieved October 4, 2022, from Stanford Graduate School of Business website: https://www.gsb.stanford.edu/faculty-research/publications/creating-value-blockchain-value-chain-management-perspective

[5] Kiran, A., Dharanikota, S., & Basava, A. (2019, October 1). Blockchain based Data Access Control using Smart Contracts. In the Proceedings of the IEEE Region 10 International Conference TENCON https://doi.org/10.1109/TENCON.2019.8929451

[6] Le, T., & Mutka, M. W. (2018, June 1). CapChain: A Privacy Preserving Access Control Framework Based on Blockchain for Pervasive Environments. In the Proceedings of the International Conference on Smart Computing (SMARTCOMP) https://doi.org/10.1109/SMARTCOMP.2018.00074

[7] Musarella, L., Buccafurri, F., Lax, G., & Russo, A. (2019). Ethereum Transaction and Smart Contracts among Secure Identities. Presented at the 2nd Distributed Ledger Technology Workshop (DLT 2019), Pisa, Italy, Feb. 12, 2019.

[8] Verifiable Credentials Data Model 1.0. (2022, March 3). Retrieved from W3.org website: https://www.w3.org/TR/vc-data-model/

[9] Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. Future Generation Computer Systems, 105, 475-491. https://doi.org/10.1016/j.future.2019.12.019

[10] ITU (2020). Recommendation ITU-T F.751.2: Reference framework for distributed ledger technologies. Retrieved, July 2022 from https://www.itu.int/rec/T-REC-F.751.2/en

[11] Gaia-X (2024). Gaia-X Architecture 24.04 Accessed August 2024 https://docs.gaia-x.eu/technical-committee/architecture-document/24.04/

[12] Gaia-X (2022). Gaia-X Trust framework 22.10 Accessed August 2024 https://docs.gaia-x.eu/policy-rules-committee/trust-framework/22.10/

[13] IDS RAM 4.0 - International Data Space Reference Architecture Model 4.0. Available at: https://docs.internationaldataspaces.org/ids-knowledgebase/v/ids-ram-4/ (Accessed 16 July 2023)

[14] Gaia-X Vision & Strategy [online]. Available at: https://gaia-x.eu/wp-content/uploads/2021/12/Vision-Strategy.pdf (Accessed, 23 July 2023).

[15] ITU (2021). Recommendation ITU-T L.1317 – Guidelines on energy efficient blockchain systems. Retrieved, September 2024 from https://www.itu.int/rec/T-REC-L.1317-202111-I

[16] F. Alam, R. Mehmood, I. Katib, N. N. Albogami and A. Albeshri, "Data Fusion and IoT for Smart Ubiquitous Environments: A Survey," *IEEE Access*, vol. 5, pp. 9533-9554, 2017, doi: 10.1109/ACCESS.2017.2697839

[17] Lau, B.P.L., Marakkalage, S.H., Zhou, Y., Hassan, N.U., Yuen, C., Zhang, M. and Tan, U-X (2019). A survey of data fusion in smart city applications, *Information Fusion*, 52, pp. 357-374, https://doi.org/10.1016/j.inffus.2019.05.004

[18] European Commission [online]. A European strategy for data. Retrieved, March 2025 from https://digital-strategy.ec.europa.eu/en/policies/strategy-data

[19] SAP (2021). Gaia-X and IDS: Usage control for data sovereignty based on SAP Business Technology Platform. Retrieved, March 2025 from https://community.sap.com/t5/technology-blogs-by-sap/gaia-x-and-ids-usage-control-for-data-sovereignty-based-on-sap-business/ba-p/13500852

[20] Tonsager, L. and Ponder, J. (2023). Privacy Frameworks for Smart Cities. *M-City*. Retrieved, March 2025 from https://mcity.umich.edu/wp-content/uploads/2023/03/Privacy-Frameworks-for-Smart-Cities_White-Paper_2023.pdf


API

For more information,
please contact: u4ssc@itu.int
Website: https://u4ssc.itu.int/

ISBN 978-92-61-40361-4

Published in Switzerland
Geneva, 2025

Photo credits: @AdobeStock