Collaborative Trusted Digital Services for Citizens

A. Luis Luis Osório, Luis Camarinha-Matos, Adam Belloum, Hamideh Afsarmanesh

▶ To cite this version:

A. Luis Luis Osório, Luis Camarinha-Matos, Adam Belloum, Hamideh Afsarmanesh. Collaborative Trusted Digital Services for Citizens. 22nd Working Conference on Virtual Enterprises (PRO-VE 2021), Nov 2021, Saint-Etienne, France. pp.212-226, 10.1007/978-3-030-85969-5_19 . emse-03338521

HAL Id: emse-03338521
https://hal-emse.ccsd.cnrs.fr/emse-03338521

Submitted on 24 Nov 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Osório A.L., Camarinha-Matos L.M., Belloum A., Afsarmanesh H. (2021) Collaborative Trusted Digital Services for Citizens. In: Camarinha-Matos L.M., Boucher X., Afsarmanesh H. (eds) Smart and Sustainable Collaborative Networks 4.0. PRO-VE 2021. IFIP Advances in Information and Communication Technology, vol 629. Springer, Cham. https://doi.org/10.1007/978-3-030-85969-5_19

Collaborative Trusted Digital Services for Citizens

A. Luis Osório[1], Luis M. Camarinha-Matos[2], Adam Belloum[3], Hamideh Afsarmanesh[3]

[1]ISEL - Instituto Superior de Engenharia de Lisboa, Instituto Politécnico de Lisboa, and POLITEC&ID, Portugal, lo@isel.ipl.pt
[2] School of Science and Technology, NOVA University of Lisbon and CTS-UNINOVA, Portugal, cam@uninova.pt
[3]University of Amsterdam (UvA), The Netherlands {a.belloum, h.afsarmanesh}@uva.nl

Abstract. In modern society, citizens aspire to get trusted and reliable digital services to authenticate theirs to payments. With the COVID-19 crisis, online shopping's fast growth has led citizens to increase registration in different systems. The registration is typically done without any guarantee that the involved business entity is trusted and that private data is managed adequately, namely according to the General Data Protection Regulation (GDPR). There are cases where online business adopts a federated authentication mechanism based on the existing and extensively adopted service providers, e.g., Facebook, and Google. With the European authorities' complacency, this de facto trend seems to contribute to a dangerous unregulated digital services model. While avoiding the centralization risks, a possible alternative is to pursue the concept of regulated and competing digital online shops or services offered under a single collaborative model across Europe. Citizens aspire to get simple mechanisms based on a single provider for authentication and pay anywhere, even with some associated costs. In this direction, we propose a model that considers regulated providers managing citizens' access to any online business in Europe, avoiding, in this way, the spreading of personal data across (business) organizations, thus decreasing the risk of personal data leaks. A collaborative network is foreseen to logically tie committed regulating authorities, providers, and digital online service providers. The proposed approach is ground on our previous research on systems integration, collaborative network infrastructure, and unified mobility payment services. This position paper offers a digital strategy for citizens, designated by Digital Person Ecosystem (DPE), which relies on Collaborative Networks concepts and centered on public authority leadership.

Keywords: Complex Informatics System of Systems, Distributed Systems, Collaborative Networks, Blockchain, Distributed Ledger

1 Introduction

There is a growing awareness of the unbalanced concentration of digital services offered by quasi-unique providers. Examples range from social networks led by Facebook, electronic commerce conducted by Amazon, Google search engine, and payments concentrated on VISA and PayPal. A table with the largest global companies in 2018 [31] from the European Parliamentary Research Service includes the first three examples in the top five companies. One main concern is that we depend on and trust that these entities do not interrupt service provision, neither do they share our private data with others [4]. Yet, the case of exploring without consent the personal data of eighty-seven million Facebook users by Cambridge-Analytics is a critical privacy failure [17]. A more recent case where Facebook banned the account of a President of one of the largest countries on the planet raises questions about the power of such private companies. In [14], the authors question the potentially harming our democracy from the current self-regulated social media. While not directly suggesting the need for public regulation, the mentioned publication somehow raises the Regulation topic. Although our research is not about political sciences, we consider being our responsibility to research collaborative models giving policymakers proper tools to act.

Our research is founded on the ISoS [24] and ECoNet [26] framework models and the collaborative mobility service provider concept [27]. The primary motivation for adopting ISoS is establishing a multi-supplier or multi-vendor technology landscape and reducing the vendor lock-in risks. Furthermore, based on ISoS, a specialized informatics system, the enterprise collaboration management system is responsible for formalizing collaboration contexts to manage interactions among organizations. Based on these technology and modeling structuring approaches, we propose a paradigm shift from the current unregulated digital business to a regulated model where Regulation Authorities play a moderation role on behalf of citizens. This paper presents and discusses the proposed change from Central Unregulated to a Decentralized Regulated model, as depicted in **Fig. 1**.

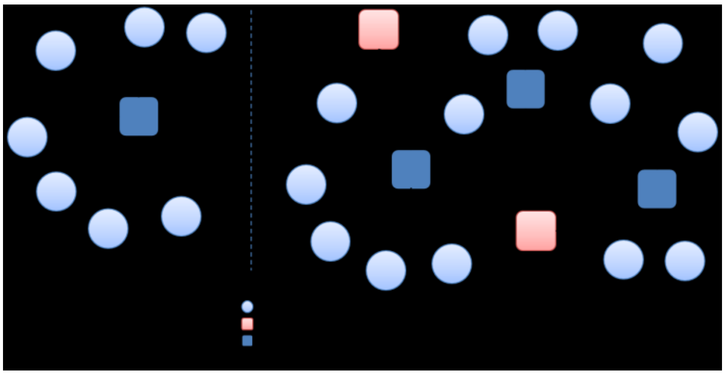

Fig. 1. Centralized and decentralized models

Evolving from the notion of collaborative mobility service provider [27], we add to the proposed provider a broader role. In other words, we assume an extension of the provider's responsibilities with an authentication service that allows citizens to log in to any regulated digital service. The idea goes beyond adopting a federated authentication as the one already offered by larger digital service providers. In our approach, the citizen uses his/her (unique) digital services provider's authentication to access any digital business, solving the current need to disperse personal data among untrusted places. We name the proposed model Digital Payment Ecosystem (DPE).

A DPE provider manages data on behalf of citizens and so the owner of the data. The provider is responsible for the technology artifacts necessary to guarantee that the citizen can maintain transaction data. Beyond controlling personal data, the objective is to eliminate the need for specific citizen accounts spread across digital providers. Federated authentication is an emerging model already adopted by private and large public digital providers, e.g., Google, Facebook. However, even if contributing to reducing accounts' spread, the existing model does not establish a generic and regulated mechanism.

While computer science and engineering theoretically have solutions making the endeavor technically feasible, the challenge is to "induce" the market towards the proposed model. There is a need for a "third force" and a convergence effort of companies and research organizations to compel consensus, what [2] calls collaborative governance. Collaborative governance defines as the mode of governance joining competing stakeholders and public agencies "*to engage in consensus-oriented decision making*." There is also a need for a novel approach to structure technology artifacts since service-oriented architectures (SOA) and, more recently, the microservices trend has been revealed to be insufficient.

Another challenge is to articulate technology artifacts involved in collaborative processes. Defining collaborative processes and activities operationalized by technology artifacts in different organizations requires coordinating execution, making transparent the heterogeneous distribution [23], [26].

The remaining of this paper is organized as follows: Section 2 presents related research work and industry contributions for the proposed endeavor. Section 3 introduces the proposed strategy for a Digital Payment Ecosystem (DPE). Section 4 describes the ISoS framework's adoption and the interactions among organizations. Finally, Section 5 presents conclusions and further research.

2 Related Research

Although no direct contributions to the mentioned challenge could be found in literature, we can find a growing concern about concentration. For instance, the concept of online manipulation is proposed and analyzed in [30] to make policymakers aware of the need to address manipulative practices systematically. Instead of focusing on privacy, the challenge is to find a strategy to strengthen the autonomy of a citizen and reduce harm for individuals and society.

The concentration of power around large technology providers is also a concern. The guidelines on outsourcing arrangements [11] published by the European Banking Authority (EBA) are discussed by Microsoft in terms of the suggested multi-cloud provider strategy, arguing that concentration already exists with on-premises mainframes [21]. Microsoft discusses the potential risks of adopting a multi-cloud approach for cloud services in the financing sector, arguing by strengthening the similarity with mainframes and the advantages of adopting a single cloud provider. Based on state of the art in complex integrated informatics systems, Microsoft might have a point here. However, the question is to weigh the risks and invest in open standards and conforming products supervised by some Competition Regulatory Authority. Our understanding is that existing dependencies are not of industry responsibility but instead of policymakers. The case of the European Court of Justice

(ECJ), judgment of the Court of First Instance (CFI) process T-201/04 - Microsoft vs. Commission where "*Decision finding infringements of Article 82 EC - Refusal of the dominant undertaking to supply and authorize the use of interoperability information*", is discussed in [18]. The interoperability issue seems to be a clear message to European policymakers to impose open standards and force European public procurement to strict conformity.

Some research works advocate that the solution for these issues is open-source. The example of Munich's municipality moving from Microsoft to Linux in 2005, named LiMux, resulted in a return to Microsoft in 2013, as reported in [19]. The report does not give any clue towards a reasonable scientific or technical explanation for the failure, and only in the article "The rise and fall of LiMux" [13] from a talk of Matthias Kirschner, President Free Software Foundation Europe (FSFE), management issues are evidenced. The retention of upgrades in some municipality departments resulted in some already corrected matters that did not become accessible to users. The question is if the suggestion of the president of FSFE appealing for lawmakers to "*implement legislation requiring that publicly financed software developed for the public sector be made publicly available under a Free and Open Source Software license*" is the right approach.

Moreover, the question is if open-source software is an adequate path to reduce concentration and at the same time contribute to the development of a competing market. The survey about free/open-source software (FOSS) developed by the Linux Foundation's Core Infrastructure Initiative (CII) shows an increase in contributors paid by their employers [16]. The trend means that companies see open source as a shared collaborative platform to value their product developments. On the other hand, the growing integration requirement makes their products better prepared to incorporate or interact with elements of other informatics systems.

While collaborative strategies to develop software libraries to incorporate as parts of systems are essential, the question is how to organize and structure enormous heterogeneous contributions consistently and reliable. Moreover, the question is how to cope with architectural complexity since companies have developed their architecture practices pulled by a fast-evolving integration pressure imposed by digitalization [20]. As a strategy to cope with architectural complexity, **Fig. 2** depicts an alternative view of the five architectures' suggested examples (Information, Process, Product, Application, and Technical). In addition, we consider the ISoS framework [24] and runtime architecture, denoting the trend for a balanced adoption of a hybrid on-premises/cloud strategy.

The authors suggest the need for a bottom-up integration of architectural domains, each with its specific language for structuring software components. In this direction, the ISoS framework unifies the diversity of architectures under the Service concept as explored in Section 4, aligned with the microservices trend [10].

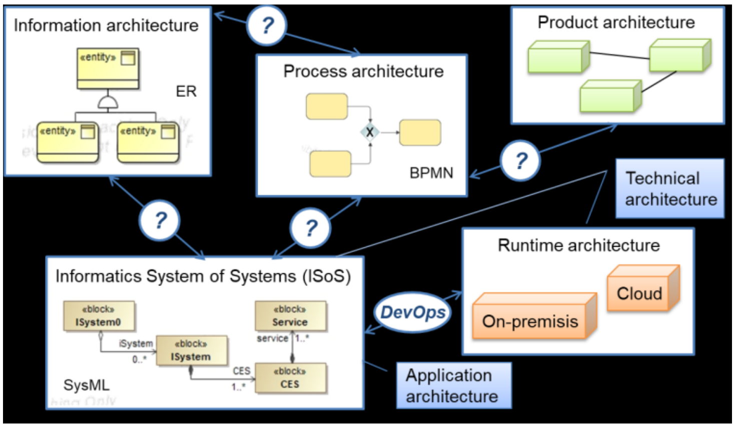

Fig. 2. The heterogeneous architecture domains adapted from [20]

Fig. 3 illustrates three specific technology architectures conceptualized, modeled, developed and deployed, maintained, and evolved under complex and critical coordination of multidisciplinary teams, commonly associated with the development and operations (DevOps) concept [32]. Despite the potential of contributing to a decentralized integration, as demonstrated in the SITL-IoT project [27], the well-known business-IT alignment remains problematic [20]. One example is the difficulty of decoupling business process logic hard-coded into applications and evolving to a business process-oriented approach adopting a standard such as BPMN [29]. Despite research efforts to adopt a complete declarative business process management system, most successful products are proprietary, e.g., the successful Outsystems[1] platform. However, there would be a clear benefit in adopting BPMN instead of a proprietary process definition language for the links marked with question marks in **Fig. 2** to be removed.

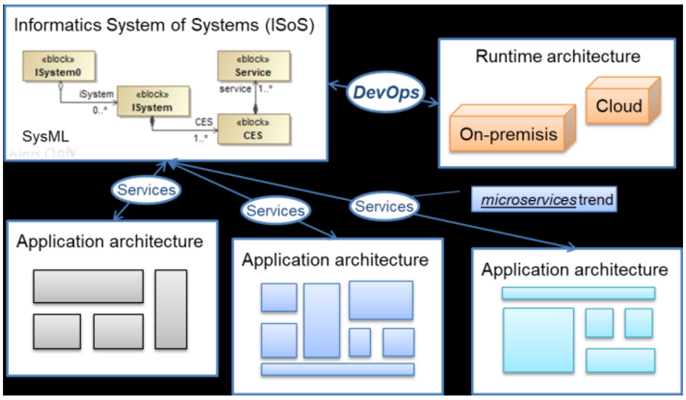

Fig. 3. ISoS hiding application architecture diversity through microservices

[1] www.outsystem.com

In the following, we present and discuss the Digital Personal Ecosystem (DPE) model, hypothesizing a modeling and technology development strategy able to contribute to a shift from the current predominantly centralized approach to decentralized digital services.

3 Model Towards a Trusted and Democratic Digital Services

The risks of citizens' control over their data is not a new concern as expressed in [8] "... *the content and software applications are only accessible online, users have no longer control over how they can access their data* ... ". The strategy followed by current large centralized providers that "… *have built successful business models around the realization that, instead of getting money in exchange for a service, it is often more valuable to provide services for free* …" is paradigmatic. Such strategy allowed them to get the network effect necessary to scale up, e.g., Google search engine, Facebook social network, or Amazon online shopping. A communication from the European Commission to the European Parliament recognizes that the fast rise of digital services, a consequence of COVID, generated dependency "… *the crisis also exposed the vulnerabilities of our digital space, its increased dependency on critical, often non-EU based, technologies* …". This sentence confirms the need for a new strategy promoting a shift from the current "concentration" to a decentralized model, involving the European industry actively, from start-ups to large corporations, in fair competition on the open global market.

A challenging question is how to address the European Commission's concern regarding the "*often non-EU based, technologies*". Previous research on a mobility payment service based on collaborative open systems defended that we need public leadership to "impose" open standards to the industry [27]. The suggestion is consistent with the US national or federal public investments to pull for consensus, motivated by integration. An example is an investment of the US Department of Defense to "*ensure a common unifying approach for the commands, military services, and defense agencies to follow in describing their various architectures*", the DoDAF/C4ISR Architecture Framework [20].

Data ownership in DPE. The proposal introduces federated authentication and citizen's ownership of the data as core services. Beyond generalizing to a pan-European payment system to pay for any digital service, a citizen would remain the data owner. To this extent, we propose adopting the distributed ledger supported by blockchain technology [4] in addiction with encryption as a strategy to manage the data generated and utilize the offered services. Moreover, the citizen maintains the prerogative of moving across providers, maintaining a continuum of access to digital services and access to private data. We name these integrated core digital services Digital Payment Ecosystem (DPE) and the regulated providers as DPE Providers.

At the start, we are concerned with payment and federated authentication (FA) services since they establish a minimal core that can contribute to revert the current concentration and give citizens the trust to access and use digital services. As discussed in previous research, the mobility service providers case was an opportunity to "impose" some convergence mechanisms led by European authorities to facilitate the development of reliable underlying technology artifacts and streamlining the integration of new services, which is still not achieved. The proposed DPE concept goes further by offering the citizen a unified mechanism to access any online service. Instead of adopting proprietary federated authentication as provided by Facebook and Google to login into any adherent site, the idea would be to restrict such service offerings to authorized DPE providers. Companies such as Facebook, Google, and any other could apply for being DPE providers and maintain their offerings. However, to get a DPE statute, they would have to comply with EU regulations imposing that a citizen client of any DPE$_x$ can log in to any of their systems with his/her authentication mechanism. In this formulation, a citizen has a unique digital identification managed by his/her selected DPE provider and can log in to any authorized (regulated) digital service by selecting his/her DPE provider among the listed ones. In this way, the online business only has access to data from the citizen (client) necessary for the business transaction. For example, a citizen with an identification managed by the DPE$_x$ provider would log in to Amazon online shop by simply selecting DPE$_x$ from the list of authorized providers listed in the online shop. After selecting check-out, the payment and access to the delivery address are under the control of his/her DPE provider. This model means that citizens have a single digital identity provider that manages their data instead of spreading registration data across multiple online businesses.

Data coordination/exchange in DPE. Furthermore, we could envisage that a DPE provider, through collaboration, could extend its core services. Adding new services requires a tight collaboration among participating business stakeholders to guarantee reliable data and coordination. Consider the example of a citizen logging in to a digital business that fails because his/her DPE provider fails for some technical reason, depending on a third party, e.g., a failure in a cloud provider, resulting in a loss. In that case, the question is which participating stakeholder shall be accountable for the potential damage.

Fig. 4 depicts the main stakeholders participating in the envisioned collaborative trusted digital services for citizens.

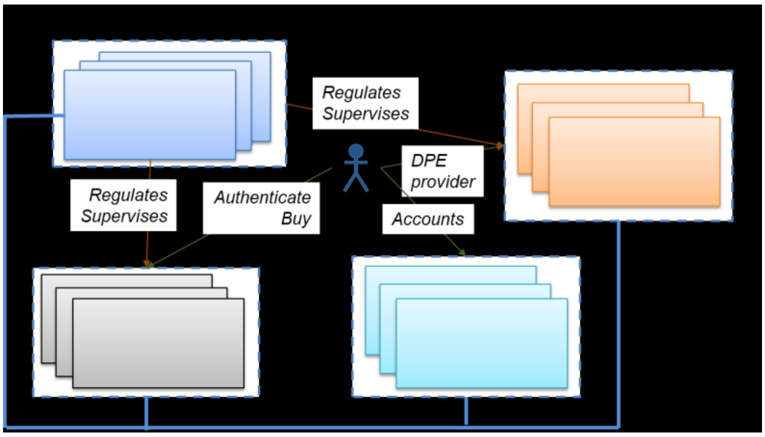

Fig. 4. The Digital Personal Ecosystem (DPE) main stakeholders

We assume that the participating organizations exchange data and coordination information through a collaborative network infrastructure. Some of the risks mentioned earlier associated with the proposed model are managed and resolved based on formal business agreements. For instance, if a login operation fails, the respective DPE provider can solve the problem. It is important to note that the model needs to be prepared to scale up. If considering only the European inhabitants, the technology artifacts need to be ready to scale up to five hundred million, based on the EU population. Engineering such networked systems are challenging since many peer businesses, and authority nodes need to reliably handle large volumes of business transactions and events per second.

The DPE provider, beyond payment that can be operationalized based on SEPA/PSD2 open specifications [12], includes federated authentication and data owned by the citizen. Federated authentication does not raise research challenges except for integration issues due to the diversity of existing single sign-on (SSO) schemes, about fourteen according to [1]. However, the mechanisms to guarantee that only the DPE customer's citizen "sees" or authorizes third parties to access parts of his/her private data raise a more complex challenge. Furthermore, the violation risk is related to the probability of potential tampering based on the robustness of the used encryption algorithm.

Data privacy and protection in DPE. In current digital services offering [15], privacy relies on the efficiency (and willingness) of providers to protect data, which can raise risks like Analytica's case [17]. Even if assuming that a provider makes the best efforts to protect data, risks depend on service providers' technology and security strategies. A possible approach considers a set of design principles known as privacy by design, as proposed in [5] and extended in [7], introducing tactics as a privacy pattern. However, given the heterogeneity and the lack of well-delimited responsibilities for the technology landscape, operations, and maintenance procedures, the proposed strategy is challenging and risky in data privacy.

Blockchain technology opens new development paths towards data privacy strategies when complemented with privacy techniques [35]. In a simplified characterization, blockchain is the glue of a distributed ledger, where linked blocks store the transactions, and peer nodes maintain a consistent replica. The addition of a new block consensus among the participating peer nodes and since the application domain is not a fiat currency but rather services for citizens, the cost of generating a block doesn't involve the concept of a miner as adopted in the bitcoin system [22]. The digital personal environment (DPE) and digital business service (DBS) providers could establish blockchain/distributed ledger to maintain business transactions. The authorities (Auth) responsible for supervising the fulfillment of regulations might also set blockchains to manage regulation/auditing events. The citizens are clients of both DPE and DBS providers and do not participate directly as blockchain nodes. However, citizens can access auth to register any complaint about any provider or access formal information about both DPE and DBS, e.g., about the accredited fact that the offered online services are authorized and supervised. The authority's role for the specialized digital business is vital for citizens to trust online digital business.

An approach to data owned by citizens could get hints from [33], which suggests a Resource Server accessed by a service provider (SP) on behalf of the End-User. The SP corresponds in our model to the DPE provider and the End-User to the citizen. We assume that blockchain infrastructures for different application domains might be heterogeneous based on different coordination strategies to persist immutable data. For example, one application domain could be the mobility payment events [27], where a mobility infrastructure agrees with dpe providers a distributed ledger store and share mobility payment events. Since the application domains refer to authorized nodes by one or more European member state authorities, the model considers the adoption of permissionless blockchains [28]. One interesting research question is how to manage the coexistence of heterogeneous blockchain implementations. The research in [28] addresses the issue of heterogeneity "*… there are a lot of frameworks, and all of them are slightly different in terms of consensus protocols …*" suggesting the need for benchmarking existing platforms. However, based on the ISoS model [18], our strategy is to assume technology diversity to make possible heterogeneous technology elements and new technologies to be adopted. Contributions to combining diverse blockchain infrastructures as the heterogeneous multi-chain Polkadot [4], the cross-blockchain communication [34], and related technologies [3] need evaluation. Beyond adopting blockchain to support distributed immutable business data, it must be guaranteed that such data are secure and available for business operation and auditing. The review [9] identifies a strong relationship between privacy and anonymization and application techniques for its implementation. However, the main research challenge is to reliably articulate organizations with their own technology culture, assuming that heterogeneity is a fact.

4 Adopting ISoS and ECoNet

The DPE model requires a reliable, complex distributed system made of heterogeneous nodes (organizations), each with its processes and technology systems. Based on a previous mobility services provider model [27], we further consider federated authentication in payment based on SEPA/PSD2 open specifications [12]. This approach is supported by the experience of 'wrapping' legacy computing technology systems, configuring a company's product portfolio under the ISoS framework. In our ISoS model, the *Service* concept models the executive elements. The *ISoS Service* concept is naturally based on the traditional Service Orientation (SOA) architecture pattern and incorporates the more recent microservice terminology. An empirical study in [10], based on industry practices in migrating legacy systems, discusses the lack of microservices architecture (MSA). One main problem is the diversity of semantics associated with Service in SOA and the more recent Microservice. While [6] argues that the microservice trend differentiates from Service/SOA, "*.. tendency can be given to the ability of independent service deploy and elastic scalability …*", the ISoS/Service has for long evolved with reliability and quality concerns. Our prior research considers reliable, collaborative mobility services as independent computing entities running on-premises or on the cloud [25]. The ISoS Service concept abstracts reliability mechanisms as an independent computing entity.

As discussed in Section 2, one possibility is to assume that the enterprise architecture of a DPE stakeholder follows the ISoS framework as depicted in **Fig. 5**.

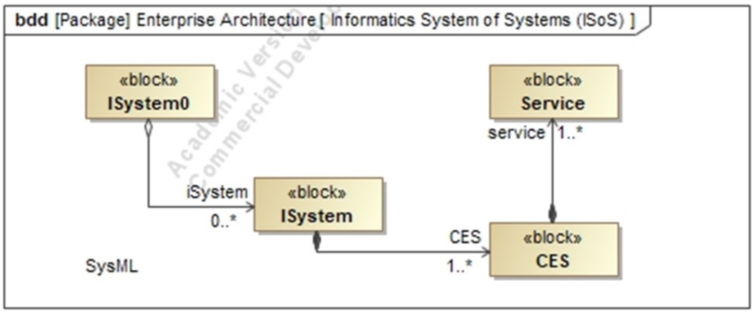

Fig. 5. The Informatics System of Systems (ISoS) framework

Any computing or communication element is modeled as a service that is part of some ISystem/CES. This simple model "unifies" the specific technology architectures, 'constructed' under diverse software development projects. Current approaches derive the architecture guided by an individual perspective of mapping problem domain requirements and technology structuration decisions. Different architects arrive for sure at different structuration of technology elements, making the resulting artifact unique. The experience of migrating an enterprise's system in the SITL-IoT project [27] suggests adopting the ISoS services framework for adapting legacy systems in the DPE context. The executive entities (Services) are, in this way, grouped in CES abstractions. Any Access to a Service entity goes through the interface zero (I_0) of the meta-informatic system $ISystem_0$. For example, to access a $Service_i$, a peer service lookups $ISystem_0$ based on a path to /$Isystem_i$/CES_i/$Service_i$ entity with the meta-data required to access the implemented functionalities. The Service instance can be running anywhere from on-premises to a cloud provider.

The results from the SITL-IoT project make us suggest a similar approach to the DPE stakeholders. Accessibility from inside or outside the organization to every Service "computational responsibility" can go through the I_0 of $System_0$. The current reference implementation of ISoS, the $ISystem_0$, adopts a REST interface accessible at isos.<organization domain>:2058 endpoint. An authorized peer computing service can access the I_0 REST interface and any implemented service through its ISystem/Ces/Service path. In other words, the $ISystem_0$ functions as a services registry, making authorized computational clients lookups for and access services.

Following a similar approach to mobility payment service, the interactions between organizations can take advantage of using the ECoNet Infrastructure [26] as formalized in [27]. For example, participation in a blockchain can be formalized as a collaboration context to share low-level secure interaction, secure communication layers, and multitenant virtual collaboration contexts.

5 Conclusions and Further Research

This position paper discusses the risks of centralizing digital services that got crescent attention by society and the research community since the Analytica/Facebook case. The "concentration" of services is related to a lack of standardization of technology systems that can reduce the risks of developing competing digital service providers and make them more accessible for authorities to supervise. The Digital Business Ecosystem (DPE) concept is a strategy to decentralize digital services. Any citizen can subscribe to a single DPE provider to access any online business with a single authentication. The DPE provider manages citizen's data under a 'blind' model as a strategy to make data safe. The authorization and regulation of any digital business (online services) motivate 'impose' a unified organization's technology architecture. Our approach for the needed unification considers adopting the Informatics System of Systems (ISoS) framework as an open specification. The ECoNet collaborative network infrastructure is proposed as a base to make data and control exchanges between organizations to share standard collaboration services.

Acknowledgments. The research conducted by GIATSI/ISEL/IPL develops in collaboration with the SOCOLNET scientific network and its ARCON-ACM initiative. The ANSR/SINCRO, BP/HORUS, and FORDESI/SITL-IoT-PT-2020 projects partially support the research. Partial support also from the Center of Technology and Systems – UNINOVA, and the Portuguese FCT Foundation (project UIDB/00066/2020), and the European Commission (project DiGiFoF).

References

1. Furkan Alaca and Paul C. van Oorschot. Comparative analysis and framework evaluating web single sign-on systems. *CoRR*, abs/1805.00094, 2018.
2. Chris Ansell and Alison Gash. Collaborative Governance in Theory and Practice. *Journal of Public Administration Research and Theory*, 18(4):543–571, 11 2007.
3. M. Borkowski, Philipp Frauenthaler, M. Sigwart, Taneli Hukkinen, Oskar Hladký, and S. Schulte. Cross-blockchain technologies : Review , state of the art , and outlook. 2019.
4. Jeff Burdges, Alfonso Cevallos, Peter Czaban, Rob Habermeier, Syed Hosseini, Fabio Lama, Handan Kilinc Alper, Ximin Luo, Fatemeh Shirazi, Alistair Stewart, and Gavin Wood. Overview of polkadot and its design considerations. May 2020.
5. Ann Cavoukian. Operationalizing privacy by design: A guide to implementing strong privacy practices. *Commun. ACM*, 55(9):7, September 2012.
6. Tomas Cerny, Michael J. Donahoo, and Jiri Pechanec. Disambiguation and comparison of soa, microservices and self-contained systems. In *Proceedings of the International Conference on Research in Adaptive and Convergent Systems*, RACS '17, page 228â€ "235, New York, NY, USA, 2017. Association for Computing Machinery.
7. M. Colesky, J. Hoepman, and C. Hillen. A critical analysis of privacy design strategies. In *2016 IEEE Security and Privacy Workshops (SPW)*, pages 33–40, May 2016.
8. Primavera De Filippi and Smari Mccarthy. Cloud Computing : Centralization and Data Sovereignty. *European Journal of Law and Technology*, 3(2), October 2012.
9. Francisco José de Haro-Olmo, Ángel Jesús Varela-Vaca, and José Antonio Álvarez Bermejo. Blockchain from the perspective of privacy and anonymisation: A systematic literature review. *Sensors*, 20(24), 2020.
10. Paolo Di Francesco, Patricia Lago, and Ivano Malavolta. Migrating towards microservice architectures: An industrial survey. In *2018 IEEE International Conference on Software Architecture (ICSA)*, pages 29–2909, 2018.
11. EBA. Final report oneba guidelines on outsourcing arrangements. web, February 2019.
12. EBF. Guidance for implementation of therevised payment services directive- psd2 guidance, December 2019.
13. Jake Edge. The rise and fall of limux, November 2017.
14. Yael Eisenstat. How to hold social media accountable for undermining democracy. Web, January 2021.

15. EuParliament. General data protection regulation (eu) 2016/679 (gdpr). Web, April 2016.
16. Hila Lifshitz-Assaf Haylee Ham Jennifer L. Hoffman Frank Nagle, David A. Wheeler. Report on the2020 fosscontributor surveythe linux foundation &the laboratory for innovation science at harvard, December 2020.
17. Margaret Hu. Cambridge analyticaâ€™s black box. *Big Data & Society*, 7, 8 2020.
18. Wolfgang Kerber and Heike Schweitzer. Interoperability in the digital economy. *JIPITEC*, 8(1):39–58, 2017.
19. KPMGtoEC. Study on open source software governance at the European Commission and selected other European institutions, 2020.
20. Marc Lankhorst. *Enterprise Architecture at Work: Modelling, Communication and Analysis*. Springer Publishing Company, Incorporated, 4th edition, 2017.
21. Microsoft. Concentration risk: Perspectives from microsoft. September 2020.
22. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, USA, 2016.
23. A. Osorio and Luis Camarinha-Matos. Towards a distributed process execution platform for collaborative networks. In: *Information Technology For Balanced Manufacturing Systems*, volume 220 of *IFIP*, pages 233–240. Springer Boston, 2006. https://doi.org/10.1007/978-0-387-36594-7_25
24. A. Luis Osorio, Adam Belloum, Afsarmanesh Hamideh, and Camarinha-Matos. Agnostic Informatics System of Systems: The Open ISoS Services Framework. In: Collaboration in a Data-Rich World. PRO-VE 2017. IFIP AICT, vol 506. Springer, Cham. https://doi.org/10.1007/978-3-319-65151-4_37
25. A. Luis Osório, Luis M. Camarinha-Matos, Hamideh Afsarmanesh, and Adam Belloum. On reliable collaborative mobility services. In: *Collaborative Networks of Cognitive Systems - 19th IFIP WG 5.5 Working Conference on Virtual Enterprises, PRO-VE 2018, Proceedings*, IFIP AICT, pages 297–311. Springer Cham, January 2018. https://doi.org/10.1007/978-3-319-99127-6_26
26. Luis A. Osorio, Luis M. Camarinha-Matos, and Hamideh Afsarmanesh. ECoNet Platform for Collaborative Logistics and Transport. In: *Risks and Resilience of Collaborative Networks*, volume 463 of *IFIP AICT*, pages 265–276. Springer, Cham. 2015. https://doi.org/10.1007/978-3-319-24141-8_24
27. A. Luis Osório, Luis M. Camarinha-Matos, Hamideh Afsarmanesh, and Adam Belloum. Towards a mobility payment service based on collaborative open systems, In: Collaborative Networks and Digital Transformation. PRO-VE 2019. IFIP AICT, vol 568. Springer, Cham. https://doi.org/10.1007/978-3-030-28464-0_33
28. Julien Polge, Jérémy Robert, and Yves Le Traon. Permissioned blockchain frameworks in the industry: A comparison. *ICT Express*, 2020.
29. Volker Stiehl. *Process-Driven Applications with BPMN*. Springer, 2014.
30. Daniel Susser, Beate Roessler, and Helen Nissenbaum. Technology, autonomy, and manipulation. *Internet Policy Review*, Volume 8(Issue 2), 6 2019.
31. Marcin SzczepaÅ" ski. Is data the new oil? Competition issues in the digital economy. January 2020.
32. Davide Taibi, Valentina Lenarduzzi, and Claus Pahl. Continuous architecting with microservices and DevOps: A systematic mapping study. *CoRR*, abs/1908.10337, 2019.
33. Nguyen Binh Truong, Kai Sun, Gyu Myoung Lee, and Yike Guo. Gdpr-compliant personal data management: A blockchain-based solution. *CoRR*, abs/1904.03038, 2019.
34. Xingtang Xiao, Zhuo Yu, Ke Xie, Shaoyong Guo, Ao Xiong, and Yong Yan. *A Multi-blockchain Architecture Supporting Cross-Blockchain Communication*, pages 592–603. 09 2020.
35. Rui Zhang, Rui Xue, and Ling Liu. Security and privacy on blockchain. *ACM Comput. Surv.*, 52(3), July 2019.