Winter 12-13-2018

AGREEMENTS FRAMEWORK FOR DATA MARKET ECOSYSTEM

Aman Sabrina Nwatchock A Koul
University of Geneva

Jean-henry Morin
University of Geneva

Follow this and additional works at: https://aisel.aisnet.org/wisp2018

Aman Sabrina Nwatchock A Koul [1]
Jean-henry Morin [2]
Department of Society Science, University of Geneva
Geneva, Switzerland,

AGREEMENTS FRAMEWORK FOR DATA MARKET ECOSYSTEM

ABSTRACT

As access to data is critically important in our society, we are witnessing the development of a data market ecosystem that supports data trade and sharing between data providers and data consumers. Intermediaries in this context are important as they provide value-added services that enable the parties to operate on the data market as they support the transactions between the main actors. In this paper, we propose an agreements framework with services enabling the collaboration between the parties together with the enabling mechanisms. It relies on a data marketplace used as a trusted third-party handling all transactions between the parties. In order to provide a high level of trust, transparency and fairness in a multi-stakeholder ecosystem, we rely on a distributed ledger approach to enable monitoring of the activities within the ecosystem as well as storing the agreements established in the data marketplace.

Keywords: Data market ecosystem; Agreement; Service, Service Level Agreement; Integrity; Non-repudiation; Transparency

---

[1] Corresponding author. amansabrina.ossey@unige.ch +41 22 379 02 57
[2] Corresponding author. jean-henry.morin@unige.ch +41 22 379 02 55

I. INTRODUCTION

Over the past few years an increasing interest toward data sharing and trade between different parties has occurred (Dong et al. 2016; Dumitru and Gatti 2016). Where any useful data of a certain domain are collected and subject to reuse, the need is likely to emerge to enable sharing of these data with potential consumers. In this context, the emergence of an ecosystem of data market adds value to data by enhancing their ability to be retrieved and distributed. Different actors may participate and offer a set of value-added services encouraging and supporting the sustainable development of such an ecosystem. Therefore, our overall research attempts to design this ecosystem with an emphasis on traceability of the exchange between actors, the respect of the principle of fairness and the right of the parties involved and finally providing tools that enable the parties to collaborate (Nwatchock A Koul and Morin 2017). In this paper, we focus on a value-added service. Namely, the data storage service enabling data owners to safely store their data to further engage in sharing them with data consumers. The data sharing process is managed by a data marketplace, a trusted third-party handling the market participants' request and managing the agreements between them. The problem we address is: how to establish a cooperative, trustworthy and transparent partnership among all stakeholders of the ecosystem (data owners, data custodians and data consumers) where data transactions remain opaque? To answer this question, we propose a design of an agreement management framework supporting cooperation among the actors. This includes describing the authorization flows among the actors based on agreements. The rest of this paper is structured as follows. Section II outlines the main services supporting the data owner activities and the associated agreements. Section III provides an agreement manager framework that supports the service execution. Section IV concludes this paper and outlines future work.

II. DATA MARKET SERVICES AND AGREEMENTS

The main parties interacting in this study are: the data owner and the data consumer. Their data sharing activities are supported by a set of intermediaries such as data custodians responsible for collecting the data owner's data under some terms defined by an agreement and the data marketplace provider managing the transactions of the main parties. We take into account the participation of data subjects as data owners and the participation of service providers responsible for the collection of a data subject's data. We assume that the service providers allow them to select a data custody service for their data storage by offering an interface, responding to a specific call of data request thanks to the portability principle of the GDPR (De Hertab et al. 2018). The data subjects will be responsible for collecting their data and bringing them to a data custody service in case there is no integration of a service provider in the data sharing process. In the ecosystem, the data marketplace serves as an intermediary upon which parties depend to create agreement and handle their transactions. This intermediary should have the following features for security and transparency support: the registration of the parties and their API before operating in the marketplace, the establishment of a secure channel between parties for communication and access token exchange and finally, the collection of the audit trail of the transactions between the parties. The added-value service is a data custody service that enables a data owner to rent data storage from a data custodian whose role is restricted to data collection and to support the data asset provisioning each time a data owner establishes an agreement with a data consumer. This service enables a data owner such as a data subject to delegate his data collection and data sharing to a third-party data custodian. It involves the creation of a storage agreement composed of the data asset description, the granularity of the data asset and the service level agreement (SLA) (Dan et al. 2004) for data collection and data

sharing. We assume that the data custodian adjusts its service offering portfolio based on global

data market demand of data access and also on the particular needs of a data consumer. The data

sharing service is a core service handled by the data marketplace. It manages the agreement life

cycle in the ecosystem and establishes the communication channel for sharing the tokens for data

access between the parties. This service is supported by a data sharing agreement composed of

the data asset definition, the usage terms and conditions of the data asset and the associated SLA

for data sharing.

III. AGREEMENTS FRAMEWORK ARCHITECTURE
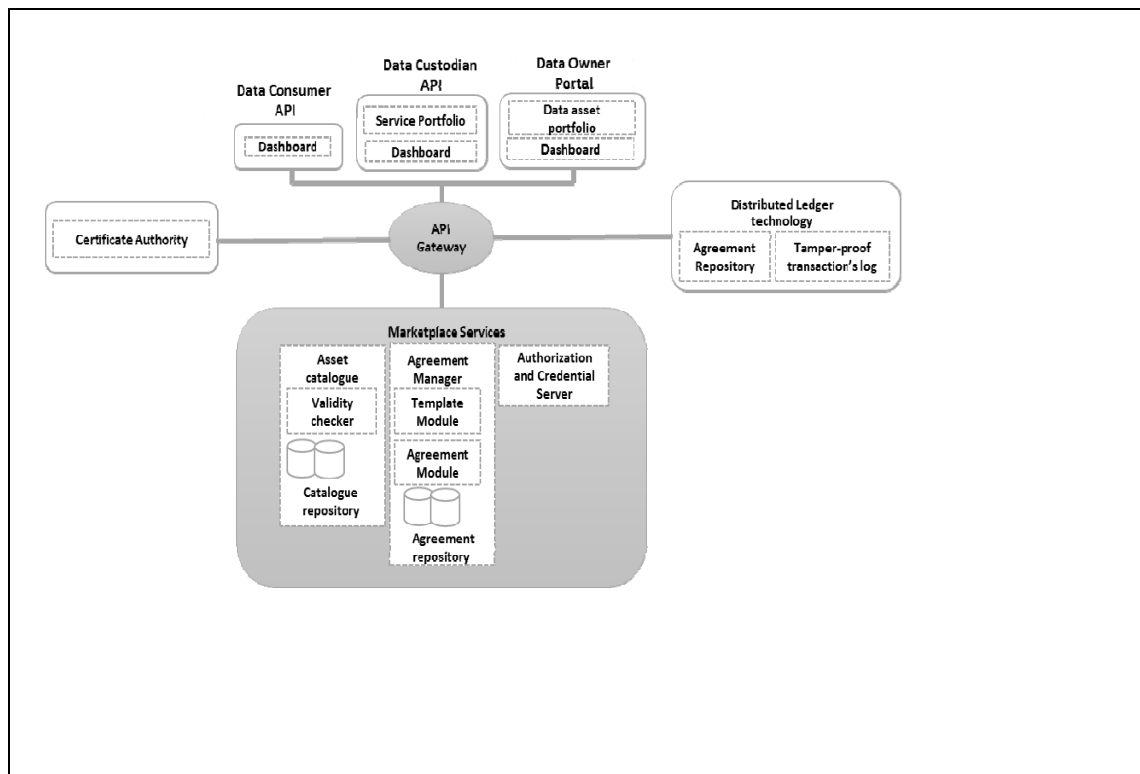
Figure 2. Agreement manager architecture

Figure 2 represents the framework for managing agreements in the data market

ecosystem. The framework consists of a set of data related services and asset discovery services,

the agreement management and the authorization server for agreement fulfillment. In addition, it

exposes an API gateway allowing the parties and the third-party API to collaborate through the

data marketplace. The marketplace integrates a DLT technology to support the agreement's integrity, non-repudiation and also the transparency of the transactions of the marketplace. As a pre-requisites, we assume that the parties have enrolled in the marketplace with a third party PKI certificate or with the marketplace authorization server and have obtained login IDs and a certificate. We describe the main components with their functionalities.

1)   The parties' portal

The parties interact with the data marketplace's services through their portal allowing them to request some services from the marketplace such as agreement creation or data access request.

2)   The asset catalogue service

It allows the registration of a data asset by the data owner and the service asset by a data custodian. A party sends his asset description for validity checks before it gets registered in the marketplace catalogue. A valid asset object is sent to the template module in order to generate the corresponding agreement template. Regarding a data asset object, the template encapsulating the agreement terms for a specific data category is generated based on reasoning over the semantic of the data asset description to propose the acceptable terms and conditions (Nwatchock A Koul and Morin 2016). In the case of a custody service, a data custodian will upload the SLA associated with the service description on the template repository. An agreement template is pre-filled based on data asset terms and conditions template and an SLA. The agreement template formulation must allow adding new properties to the template. The pre-filled agreement template is submitted to the agreement manager for recording in the agreement template repository. The asset offering is then saved into the catalogue repository with the link to the agreement template.

3)   Agreement execution between a data provider and a data custodian

Figure 3 shows a flow diagram for data storage agreement fulfillment process between data providers, data custodians and the service provider. In this model, we assume that the data custodian and the data owner have negotiated an agreement based on the custody service offering and have accepted the agreements terms and conditions. Every transaction is managed by the marketplace authorization server which based on the agreement between the parties responds to their data access request and transmit the access token, thus allowing a single point of transaction log record.
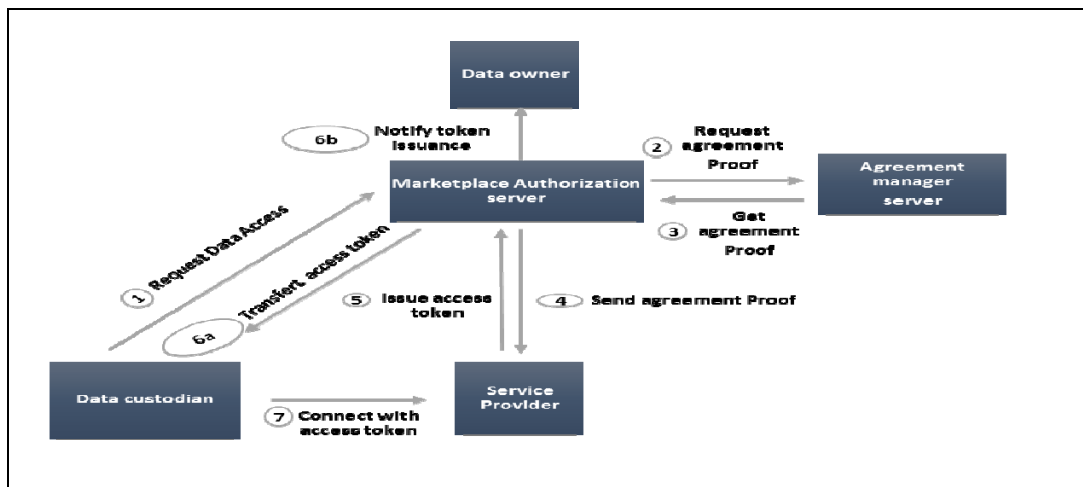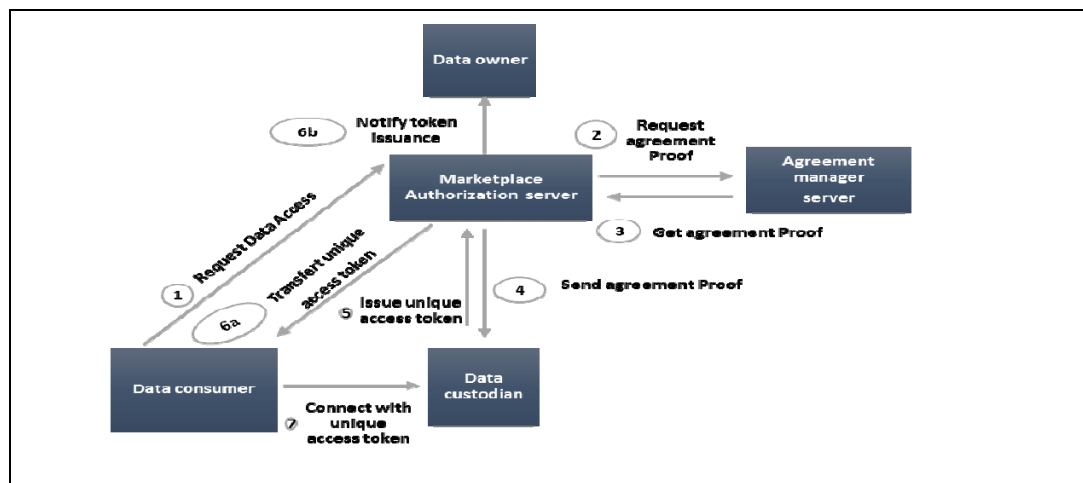

Figure 3. Agreement execution flow between a data provider and a data custodian

4)   Agreement execution between a data provider and a data consumer

Figure 4. Agreement execution flow between a data provider and a data consumer

Figure 4 shows a flow diagram for data access agreement fulfillment process between the data consumers, the date owner and the data custodian. Once again, the marketplace authorization manager handles the request of the parties. The data consumers rely on the marketplace to get one-time tokens generated for each data access request from the data custodians. The token encapsulates the rights that a data owner delegates to a data consumer, so that they have granular access to data asset.

5) Distributed ledger for agreement proof and audit trail

The DLT integration provides an option for ensuring the integrity of an agreement and non-repudiation of the parties (Xu et al. 2016) in environment relying on intermediation. A party may deceive another party about the agreement terms. Therefore, a party may request the use of a DLT as trusted service. The agreement and its hash will be used as a proof to check the authenticity of both parties agreement. Thus, the marketplace will be responsible for creating a transaction block with the agreement and its hash automatically in a DLT just after the agreement creation. The parties involved in the agreement will endorse the validation of the block after checking the authenticity of the agreement. The agreement manager may get the references of each block created for a specific agreement hash and send it to the parties involved in order to facilitate the search of an agreement. Hence, the marketplace will ensure the transparency of the transactions among the parties.

IV. CONCLUSION

In this paper, we have described some specific services supporting data trade and sharing in a data market ecosystem and an agreement framework for handing agreements between some market participants. While technological advances enables disintermediation in data sharing and

trade, we define instances where the intermediaries like the data marketplace provider, the data custodian are necessary as they provided specific values to market participants. However, their success lies in their ability to provide transparency, trust and fairness in handling data and transaction. This study addresses a specific part of the more general research issue dealing with the design of a fair and responsible data market ecosystem. Our Future work will cover the integration of this agreement framework within the full reference implementation and a corresponding real case pilot.

REFERENCES

Dan, A., Davis, D., Kearney, R., Keller, A., King, R., Kuebler, D., Ludwig, H., Polan, M., Spreitzer, M., and Youssef, A. 2004 "Web services on demand: WSLA-driven automated management," IBM Syst. J., vol. 43, no. 1, pp. 136–158.

De Hertab, P., Papakonstantinoua, V., Malgieria, B., and Sanchezc, I. 2018. "The right to data portability in the GDPR: Towards user-centric interoperability of digital services," Computer Law & Security Review, Volume 34, Issue 2, Pages 193-203.

Dong, X., Guo, B., Duan, X., Shen, Y., Zhang. H., and Shen, Y. 2016 "DSPM: A Platform for Personal Data Share and Privacy Protect Based on Metadata," 13th International Conference on Embedded Software and Systems (ICESS); DOI: 10.1109/ICESS.2016.10; ISBN: 978-1-5090-3727-8.

Dumitru, R., and Gatti, S. 2016. "Towards a reference architecture for trusted data marketplaces: the credit scoring perspective," In Irfan Awan and Muhammad Younas, editors, 2nd International Conference on Open and Big Data, OBD 2016, Vienna, Austria, pages 95-101, IEEE Computer Society, 2016. 10.1109/OBD.2016.21.

Nwatchock A Koul, A. S., and Morin, J-H. 2016. "Towards a Taxonomy of Data and Guiding Principles for Data Markets," Proceedings of the 11th Pre-ICIS Workshop on Information Security and Privacy, Dublin, Ireland.

Nwatchock A Koul, A. S., and Morin, J-H. 2017. "Towards a framework for a fair and sustainable data market ecosystem," Proceedings of the 12th Pre-ICIS Workshop on Information Security and Privacy, Seoul, South Korea.

Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A. B., and Chen, S. 2016. "The blockchain as a software connector," 13th Working IEEE/IFIP Conference on Software Architecture.