

The JLINC protocol of the present invention enables a more secure and flexible solution that addresses the requirements of both PSD2 and GDPR. The following is a description of the JLINC protocol as it applies to a three-party interaction:

The three actors involved in the system and implementation of the present invention, and their interacting cloud services, per an example interaction, are as follows:

- The Bank, referenced as “BankCo”.
- The bank’s agent, the BankCo JLINC Solutions Service.
- The Financial Technology company, referenced as “FinCo”.
- The Financial Technology company’s agent, the FinCo JLINC Solutions Service.
- The end-user, the “data subject” in GDPR terms, or “resource owner” in OAuth terms, referenced as “Alice.”
- Her agent is the JLINC Data Service, which she accesses via her JLINC App.

The interaction of the three parties can be seen in FIG. 5

Alice can be initially onboarded to the system of the present invention (JLINC) via either BankCo or FinCo. For this discussion example, it is assumed she is being onboarded by BankCo, but the process is the identical, regardless of how Alice is onboarded to the system.

BankCo initializes each existing or new customer on its JLINC Solutions Service by sending the customer’s account number or other ID that uniquely identifies the customer in the bank’s records to the appropriate JLINC Solutions Service API. Then, the process is as follows:

CLAIMS

We claim:

1. A method for data usage control, comprising:

using one or more computer processors:

automatically granting tailored permission related to use of a first party's data and related to transference of the first party's data between databases; and

establishing a cryptographically signed Information Sharing Agreement (ISA) between the first party and one or more other parties, the ISA providing the tailored permission;

wherein the ISA allows and governs automated data exchange, between the first party and the one or more other parties, of the first party's data, and wherein the ISA allows and governs automated data exchange, between the one or more other parties and one or more additional parties, of the first party's data.

2. The method of claim 1, further comprising, using the one or more computer processors, serving one or more advertisements to the first party according to first party preferences.

3. The method of claim 2, wherein the ISA includes the first party preferences, and wherein the first party preferences govern one or more aspects of advertisements allowed to be served to the first party.

4. The method of claim 1, wherein the ISA is established using a graph language.

5. A method for data usage control, comprising:
 - using one or more computer processors:
 - displaying, on a computing device, a data control selector;
 - receiving selection of the data control selector from a first party of a plurality of parties;
 - in response to selection of the data control selector, initiating display of one or more data control user interfaces;
 - receiving one or more user inputs at the one or more data control user interfaces, the one or more user inputs indicating first party preferences related to usage of the first party's data;
 - establishing an Information Sharing Agreement (ISA) between the first party and one or more other parties of the plurality of parties, using the indicated first party preferences, the ISA governing usage of the first party's data;
 - generating a hash of the ISA;
 - adding cryptographic signatures to the hash from the first party and the one or more other parties, thereby establishing a cryptographically signed hash which validates a finalized ISA, wherein the cryptographically signed hash comprises the hash and the cryptographic signatures;
 - providing the cryptographically signed hash to the first party and the one or more other parties; and
 - wherein the first party's data is transferred to the one or more other parties only after the finalized ISA is established.
6. The method of claim 5, wherein the finalized ISA governs which entities may collect or obtain the first party's data, which of the first party's data can be collected or obtained, and what acts entities are allowed to do using the first party's data.
7. The method of claim 5, wherein the finalized ISA is established automatically and is automatically cryptographically signed using an automated software agent without requiring manual signatures.
8. The method of claim 5, wherein terms of the finalized ISA are perpetuated

automatically by a new party being required to cryptographically sign the finalized ISA before receiving the first party's data from one of the one or more other parties.

9. The method of claim 5, further comprising capturing and storing a hashed audit record of all data events of the first party's data, signed by each of the other parties who have participated in any of the data events, to establish one or more chains of custody of the first party's data.

10. The method of claim 9, further comprising receiving and storing, by a software agent associated with one of the parties of the plurality of parties, a record of each data event in which that party has participated.

11. The method of claim 5, wherein the finalized ISA is expressed in JSON-LD.

12. The method of claim 5, further comprising restricting or withdrawing a previously-allowed usage of the first party's data, as allowed by terms of the finalized ISA, in response to one or more selections from the first party.

13. The method of claim 5, further comprising receiving an indication of an audit service from the first party and each of the one or more other parties, and providing a signed record of data events associated with the finalized ISA to the audit service of each party of the plurality of parties.

14. The method of claim 5, further comprising verifying one of an age of the first party, an identification of the first party, a location of the first party, and a verifiable attribute of the first party, and wherein the first party's data is transferred to the one or more other parties only after the verification has occurred.

15. The method of claim 14, wherein the verification is provided by a countersigner who is not the first party, the countersigner countersigning with a key, and wherein an identity attribute of the first party is not provided so that the first party remains anonymous.

16. The method of claim 5, wherein the first party's data is automatically generated by an IoT device.

17. The method of claim 5, wherein one of the one or more other parties comprises a device.

18. A data usage control system, comprising:

a data control selector displayed on a first computing device, the data control selector configured to initiate display of one or more data control user interfaces configured to receive one or more first party inputs indicating the first party's preferences related to usage of the first party's data; and

one or more servers communicatively coupled with the computing device and configured to:

store, in one or more data stores, in response to receiving the one or more user inputs, the indicated first party preferences;

establish an Information Sharing Agreement (ISA) between the first party and one or more other parties, using the indicated first party preferences, the ISA governing usage of the first party's data; and

generate a hash of the ISA;

add cryptographic signatures to the hash from the first party and the one or more other parties, thereby establishing a cryptographically signed hash which validates a finalized ISA, wherein the cryptographically signed hash comprises the hash and the cryptographic signatures;

providing the cryptographically signed hash to the first party and the one or more other parties; and

wherein the ISA facilitates automatic usage of the first party's data by the one or more other parties or transfer of the first party's data to the one or more other parties, in response to one or more of the following triggers: arrival of a date; arrival of a time; alignment of financing terms between the first party and the one or more other parties; alignment of price between the first party and the one or more other parties; and alignment of a product or service requested by the first party and a product or service able to be provided by the one or more other parties.

19. The system of claim 18, wherein the ISA further facilitates an automatic financial transaction between the first party and one of the one or more other parties in response to one or more of the triggers.

20. A method for online contractual validation, comprising:
- using one or more computer processors:
 - generating a hash of a draft contract;
 - using one or more user interfaces, adding cryptographic signatures to the hash from a first party and one or more other parties, thereby establishing a cryptographically signed hash which validates a finalized contract, wherein the cryptographically signed hash comprises the hash and the cryptographic signatures;
 - providing the cryptographically signed hash to the first party and the one or more other parties; and
 - receiving an indication of an audit service from the first party and each of the one or more other parties, and providing the cryptographically signed hash to the audit services of the first party and the one or more other parties;
- wherein the finalized contract does not govern an exchange of data between the first party and the one or more other parties.