Secured and efficient information exchanges in collaborative networks: the Singular Information System

Cédrik Béler[1] and Bernard Grabot[1] ,

[1] Université Fédérale de Toulouse Midi-Pyrénées, LGP-ENIT-INPT
47 Avenue d'Azereix, BP 1629F-65016 Tarbes Cedex, France
{cedrik.beler, bernard.grabot}@enit.fr

Abstract. Information exchange is the object of intensive research from quite separated communities, dealing for instance with connected objects, interoperability of industrial information systems, personal information systems or data security. A unified framework, defining the conditions of interrelations of elementary information systems, could allow to address these problems with a holistic view. In that purpose, we suggest the concept of Singular Information System (SIS) and give the basic principles allowing the connection of two SIS. We show then how exchanges of information between objects, persons and organizations may benefit from such a unified paradigm.

Keywords: Information system, personal information system, collaboration, interoperability.

1 Context: Information sharing in collaborative networks

Collaborative Networks (CN), i.e. networks of autonomous organizations that collaborate to better achieve common or compatible goals [1], are now considered as the best solution for coping with the uncertainty of the markets and with an increased competition. For a company, the interest to belong to such networks is to extend its competences and share risks, allowing to benefit from opportunities that the company could not address alone. Information sharing is quite commonly considered as an essential condition for maintaining collaborative relationship between partners [2]. What information should be shared and how is an important problem for long-term relationships, but becomes critical when organizations want to create a short term relationship. In this context, the mass of digital information created today by individuals, organizations and connected objects may result in an uncontrolled flow of information. Breaches in confidentiality and inefficient communication, resulting in an increased risk, are possible consequences in collaborative networks. A reason of this situation is that even if the interoperability of organization's information systems, personal information systems and connected objects are "hot" topics now, no framework has yet been proposed that would provide a unified, secured, centralized and controlled way for exchanging information between "carriers of information" of different levels. To the difference with many works focusing on the interoperability of the information systems of organizations, we suggest choosing as central component the dedicated and private information system of an entity (object, individual or

organization), that we call the *Singular Information System (SIS)*. The qualifying term "singular" was chosen to strongly underline the uniqueness of such IS. SIS are owned by only one entity and contains only information the entity wants to store in a secure and private manner. Therefore, each SIS is singular by its content and by its nature. Collaboration between SIS is achieved through their interconnection resulting in (singular) information transactions.

The aim of this communication is to present this prospective work by explaining the basic principles allowing SIS to communicate, focusing here on applications linked to collaborative networks.

2 Related works: from collaborative organizations to singular information systems

The interest of process modeling for describing the internal behavior of an organization is now universally recognized. Comprehensive modeling tools like ARIS [3] allow to link process activities to the organizational elements performing these activities (services, departments), then to persons belonging to these elements of organization. It is not anymore enough: many papers have shown the interest of building communities for taking benefit from external experience, within or outside the company. The success of professional social networks is an illustration of this new propensity [4]. In that case, the distinction between the individual and professional social networks may become unclear. Therefore, there is in our opinion a need for clearly defining a personal information system, and investigating how it feeds personal or professional "consumers of information" in a controlled way, respecting the basic principle that personal data may be used by external entities only under permission. The page of an individual or organization in a social network can be considered as an embryonic SIS regarding the functionalities but most of the time, control and privacy are not guaranteed. Clarifying the relationships between a person and an organization is not the single utilization of SIS: "connected" or "intelligent" objects [5] will be more and more present in companies. Their embedded simplified information system may also be considered as a SIS, and their relationship with the SIS of persons and organizations may be managed according to the same principles. So, the SIS can be considered as the private information system of an entity (object, individual or organization), allowing the entity to keep control over all information transactions in which it is involved. In this paper, only the personal and organizational level is tackled.

The idea of personal information system is not new. Vannevar Bush's 1945 Memex vision (namely memory extender) was the description of an analogical computer where people could store and link information together [6]. Recently, an implementation of Memex was realized with MyLifeBits [7], a lifetime store of everything a person could encounter in his life. These systems are limited to person and do not enable collaboration. Recent considerations of the problems related to information dissemination have raised a new literature related to personal information systems. Ann Cavoukian [8] proposes for instance a new paradigm called Privacy By Design (PbD) that aim at considering privacy as the raw building block of an information system. Close to this point of view are alternative social network tools

distributed as open-source solutions, built with privacy as first principle (e.g. Diaspora [9], Heartbeat [10] or Safebook [11]). Interesting works on the development of personal information systems, called Personal Data Store/Server (PDS), Personal Data Vaults/locker (PDV) or Personal Cloud, can also be found [8]. Some recent initiatives (Mydex [12], Meeco [13], sdX [14], etc.) share the same goals of data storage and exchange security and privacy with different design choices. Even if these tools are said to facilitate information exchange, they essentially focus on data storage and data aggregation, and stay essentially at a personal level (even if some of them, like Meeco or Mydex, include the relationship of the customer with organizations).

Several works focus on the collaborative aspects of information exchange in organizations and are by the way good inspirations even if they do not consider persons as a first principle which is essential to us. Besides all works on Collaborative Information Systems ensuring interoperability between several exogenous IS, let us note one initiative. Federated Information System [15] is the evolution of federated database system which is a multi-database system in which every node in the federation maintains its autonomy on the data. A set of export schemas (derived from local schemas) through which the data is made available to other specific nodes are the underlying working principle. The way information is exchanged is interesting but the SIS approach is more global and not limited to a given context. Instead of exporting internal IS database models, SIS rely on messaging between SIS according to a given protocol ideally without considering IS internals. Moreover, the unicity of a person, an organization is again not considered.

Another recent tendency is BYOD (Bring Your Own Device) in cloud environments allowing people to bring and use their own devices in work contexts. Indeed, personal devices (smartphones, tablets, …) associated to Cloud environment and smart assistant (like Apple or Google ecosystems) tend to be potential SIS but they have inherent limitations (business model based on data disclosure or proprietary model without guarantee in the long term). More over, BYOD is a rather practical approach that raises several security issues [16] and promotes the multiplication of entry points which is clearly in opposition to what SIS envisions.

Finally, some other recent researches fostered around the idea of privacy exchange of information seem to be good foundations for the development of SIS. The Minimum Exposure Project [17] aims at controlling information sharing and capitalization for an entity both in input (filtering data input) or output (data exposure frequency and duration). This underlying limited data collection principle seems essential to limit the dissemination of information (a well known privacy principle) but also to have a fine control on incoming information. Also, Trusted Cells as component of smart objects (trusted devices) are an interesting approach to ensure privacy relevant application [18]. Finally, asymmetric architectures like MetaP have been suggested for connecting secured and unsecured networks [19] and could be of high interested to interconnect SIS through Internet.

In the next sections are defined SIS principles and abstract models so as to show how interconnected SIS can improve agility of CN and therefore their resilience regarding communication inefficiencies.

3 SIS architecture and principles

A SIS is a private and dedicated information system that would be the unique place where is recorded the whole "digital life" of an entity (object, individual, organization, network of organizations, government...). It has the ambition to provide a scalable framework able to link individuals, smart objects and organizations. As a consequence, the required global functionalities of a SIS should be:

- global querying and data/information/knowledge mining,
- anonymous data publishing,
- distributed secure sharing (users must get a certified proof of legitimacy for the credentials exposed by the participants of a data exchange eventually using a third-party),
- secure usage and accountability (users must not loose control over their data through data sharing),
- service offering or acceptation (local push opportunities, ads, love market,…),
- collaboration facilities (automatic update of information about other SIS, distributed planning of collaborative processes between SIS partners…).

The core of the system is the private information stream (life data stream) capturing each piece of information (data, pictures, videos...) that the singular entity wants to store. All recorded information is private by default, leveraging todays legal limitations of classical IS to store personal information, according to the PbD principles. A "view" on the SIS can be created for a certified partner, according to the respective roles of the entity and its partner. Several SIS, when interconnected, define a network of SIS called INTERSIS (Interconnection of Singular Systems).

SIS dedicated to persons, organizations or objects share the same architecture. Conceptually, a SIS is composed of a private core and of information views extracted from the private core to structure information of interest, used internally or shared with other SIS. Private core singular information must only be accessible by his owner and contains only singular information.

Singular information structuration is important to be able to do generic lookup on past information, but also to perform information and knowledge inference at the owning entity level (assistant dimension of SIS). Singular information (SInfo) can be considered as a personal digital trace and is essentially a wrapper on usual kind of data (structured or unstructured data, files, applications logs...). Meta information is added in a generic manner (geospatial and temporal information on the information input, with an extensive use of tags that express the context of the information). Useful information can be added in an information container without being conformant to a data model. SInfo have several properties: they can be composed forming a tree where leafs are raw types (composition), evolution and history must be accessible (versioning), several variations may represent the same information according to different detail level (variation) and one SInfo could be the synthesis of several others (synthesis). Raw types may be text, picture, video, sound, website snapshot… An information view is a particular kind of SInfo that may be dynamic (for example, the age of a person could be a view extracted from his singular information “date of birth’’). Singular information views and singular information

structuration will be deeper studied in future works so as to validate its universality and scalability.

Collaborative dimensions are managed through SIS interconnections. For such purposes, SIS basic structure includes collections of persons, organizations and objects/resources with which the owner has authorized exchanges of information in given situations. Information exchange is materialized by singular information transactions and consists in: 1) extracting a view from singular information, 2) defining the term and conditions of the exchange (limited data collection principle) and 3) establishing the transaction according to a secured communication protocol.

Several types of interactions are possible. The first kind is the exploitation of the SIS itself by the owning entity (information mining, digital assistance…). Other kinds of interaction may be defined depending on the entities that are engaged in any singular information transaction. There are transactions between similar entities: a) person to person (PtP), b) organization to organization (BtB), c) object to object (OtO) and transactions between different kinds of entity: d) person to organization (PtB), e) person to object (PtO) and f) object to organization (OtB). Each of these interaction classes is a potential CN use case, but the most important are BtB and PtB, the former underlying each potential collaborative role in the supply chain for instance, while the latter implements each potential role a person can have regarding an organization.

Of course, it is not reasonable to imagine that every organization and person on earth would adopt at short term the SIS paradigm and this is why one major requirement of SIS is the interoperability with legacy IS (for people, organizations and smart objects). Moreover, although the basic idea is to interconnect SIS, it is not viable to imagine an always-connected system, hence SIS has to “work offline”. Eventually, SIS could be most of the time disconnected, only initiating a communication when necessary, without being connected to an unsecured network like Internet (e.g. if a person wants to exchange information with an organization like a hospital, the connection can be done physically). SIS "proxies" can be introduced as a mean to deal with non universality and sporadic connections. A proxy is a classic pattern in computer science, whose intent is to provide a surrogate for another object to control access on it. They can be considered as “smart and authorized views” on external information systems associated to objects, persons, and organizations. Actually, a SIS owner can "see" what another entity “sees” of itself by exploring its associated proxy (however he has no clue on what was filtered). When disconnected, a SIS proxy acts as a non-synchronized system. It can represent entities that are not SIS (legacy system for which bridges can be developed) but also non-connected SIS. SIS proxies, when interconnected, have of course much more potential. This connection is necessary to establish/resume information transactions, which is the core functionality of INTERSIS. Also, to deal with the sporadic functionalities, information transactions have to be asynchronous, i.e. there can be pending transaction, initiated when disconnected, and resumed once connected. Information update is done only when all SIS engaged in a transaction are connected.

Defining a proper communication protocol so as to meet the requirements of singular information transactions will be a very important challenge in future works.

4 Collaboration through SIS

In this section, more details are given on the organizational SIS, and a collaborative use case is introduced through a planning assistance tool.

Imagining SIS for persons and objects is more straightforward than for organizations because of the complex nature of an organization (composed of services, departments and ending with persons). An organization has a main global SIS but also includes a composition of other SIS: several organizational SIS reflecting its organization (companies, subsidiaries, services, working group…), several personal SIS according to the role of persons (governance, employees, stockholder, final customers…) and several SIS for objects of interest (resources that are shared and smart objects). One important aspect to consider is that personal SIS is the main entry point for organizational SIS (for instance, a CEO access his organizational SIS through his personal SIS). The organizational SIS can be more volatile than the organization structure, i.e. it can be created on the fly according to a specific task that needs a specific organization (project group for instance). When the task is over, the SIS is dismantled and absorbed by the parent SIS. By default, it is possible to include all SInfo of the former SIS, but clever inclusions can be done depending on what lesson learned are interesting to store (is it the result of the project or eventually the process followed that we are interested in?). Temporary creations of organizational SIS are also possible for working groups that are a federation of people and/or organizations (i.e. outside an organization perimeter).

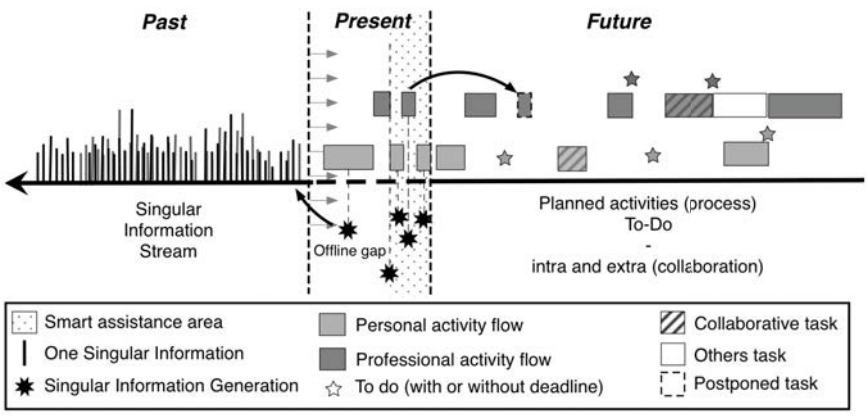

Fig. 1. SIS Timeline Paradigm applied to planning

To illustrate the collaboration facilities that SIS provide, one major tool is the planning assistant, which is a basic but very important application of all SIS. Its functioning is illustrated on Fig. 1 and rests on the SIS Timeline Paradigm that serves as support to plug applications to one SIS. The SIS internal architecture makes a clear distinction between three temporal dimensions: past, present and future. SIS is primarily a unified communication framework but its first purpose is to help organization, so this temporal distinction is very useful in that respect. The past dimension is about storing the singular information stream to reuse it later (global

querying, information view creation/extraction…). Storing SInfo is an important requirement and so as to ensure privacy and control, it is possible to choose between different providers (todays encrypted cloud services for instance).

"Present" corresponds to the basic usage of a SIS and consists in the conversion of future planned activities to digital traces stored as singular information belonging to the “past” dimension. Coupling between future activities and current activity could be of great assistance to infer and classify automatically new SInfo. Let us remark that singular information is not always converted from a planned activity. Indeed, an activity can start without being planned. Fig. 1 also symbolized activity treatments that result always in new SInfo (one that can be a summary of the activity done, or one logging the fact that the activity was postponed or cancelled).

One important aspect of the present dimension is the "offline gap", meaning some activities or tasks may be started when the SIS is not used. So when resuming a SIS, each application has to provide facilities to roll out the timeline until the last usage so as to give the possibility to enter SInfo asynchronously as if it was done inline.

"Future" is mainly about planning tasks. In todays world, it is a real challenge to reconcile our career and private life. Applying SIS to planning through singular information transactions seems promising as it enables an up-to-date and efficient view on every planning of interest (personal, organizational…). Of course, this is possible if you have an authorized (full or restricted) view on another SIS planning. On Fig. 1 is depicted a personal and a professional activity flows. Note that there are potentially as many activity flows as you have personal/object SIS. The limited data collection principle applies here too. One can decide to share only some activities with some persons or some organizations or to share free time intervals on specific durations. One can set up an activity that engage someone else and, once accepted, he will be notified in near real time on all possible (authorized) evolutions. For instance, somebody can assign a task to you and it will appear in your planning. Once started, the responsible could know if it is started (if you have authorized this transaction) and once finished, the responsible could receive specific information like the time spent on the activity, eventual encountered problems, etc. Again the power of SIS is that you send only what is needed or what you think is relevant. Nothing prevent yourself from recording lots of information and keeping most of them private at the end.

5 Conclusion and perspectives

The uncontrolled access of information created by the daily life of individuals and organizations clearly set confidentiality and efficiency problems. The first elements of Singular Information System have been described in this communication, with the aim to give to each entity a permanent control on its digital information, while increasing the interoperability between entities, which seems to be now a non negotiable requirement of our modern life. We strongly believe such systems would greatly enhance the agility of collaborative networks by improving reactivity.

Having one logical entry point per entity aggregating all life information exchanges regardless their context (personal(s), professional(s), …) is according to us an important foundation to cope with today explosion of data exchanges: it

considerably leverages interoperability and complexity issues while preserving privacy. Of course, this require a strong paradigm shift which could be considered infeasible as one may think that everybody, every organization, every smarts objects should embrace this paradigm to succeed. Of course, this is not the purpose of SIS and this why we envision SIS proxies as a way to manage under the same interfaces legacy IS and SIS.

As a prospective work, SIS approach needs several additional developments and refinements. Next step will be the development of personal SIS applied in the context of SME so as to share productivity information (processes, activities, …) between a project manager and employees. In the same time, theoretical developments will be conduced regarding singular information structuration and information transaction definition (as the underlying communication protocol).

References

1. Camarinha-Matos, L.M., Afsarmanesh, H.: Collaborative networks: A new scientific discipline. Journal of Intelligent Manufacturing, 16(4-5), 439--452 (2005)
2. Nyaga, G.N., Whipple, J.M., Lynch, D.F.: Examining supply chain relationship: Do buyer and supplier perspectives on collaborative relationships differ. Journal of Operations Management, 28, 101-114 (2010)
3. Scheer, A.W.: *ARIS: Business Process Modeling*, Springer (2000)
4. Grabot, B., Mayère, A., Lauroua, F., Houé, R.: ERP 2.0, what for and how? Computers in Industry. 65(6), 976–1000 (2014)
5. Meyer, G.G., Främling, K. and Holmström, J.: Intelligent Products: A survey. Computers in Industry, 60 (3), 137--148 (2009)
6. Bush, V.: As We May Think. The Atlantic. Reprinted in Life magazine (1945)
7. Gemmell, J., Bell, G., Lueder, R., Drucker, S., Wong, C.: MyLifeBits: Fulfilling the Memex Vision. ACM Multimedia, Juan-les-Pins, France, 235—238 (2002)
8. Cavoukian, A.: A privacy by design approach to an individual pursuit of radical control. Digital Enlightenment Yearbook: The Value of Personal Data, IOS Press, 89--101. (2013)
9. Diaspora*, https://diasporafoundation.org
10. Heartbeat, https://ind.ie
11. Cutillo L., Molva , R., Strufe, T.: Safebook: A privacy-preserving online social network leveraging on real-life trust. IEEE Communications Magazine, vol. 47(12), 94--101 (2009)
12. Mydex, https://mydex.org
13. Meeco - sovereignty for all, https://meeco.me
14. sdX: the building blocks of small data apps, http://smalldata.io/#sdx
15. Afsarmanesh, H., Camarinha-Matos, L.M.: Federated Information Management for Cooperative Information. In: 8th Int. Conf. on Database and Expert Systems Applications (1997)
16. Morrow, B.: BYOD security challenges: control and protect your most sensitive data. Network Security, vol. 2012 (12), pp. 5--8 (2012)
17. Anciaux, N., Nguyen, B., Vazirgiannis, M.: The Minimum Exposure Project: Limiting Data Collection in Online Forms, in ERCIM News, vol. 90, pp. 41--42 (2012)
18. Anciaux, N., Bonnet, P., Bouganim, L., Nguyen, B., Popa, I., Pucheral, P.: Trusted Cells: A Sea Change for Personal Data Services. In: 6th Biennial Conference on Innovative Database Research (CIDR) (2013)
19. Allard, T., Nguyen, B., Pucheral, P.: METAP : Revisiting Privacy-Preserving Data Publishing using Secure Devices. In: Distributed and Parallel Databases (DAPD) (2013)