

Position paper for W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement

“Privacy languages from a telco operator perspective”

Susana Jurado-Apruzzese, Francisco J. Garijo-Mazario and José Sánchez-Sánchez

Telefónica I+D

Tel: +34 91 337 {4414, 4235, 4331}, Fax: +34 91 510 3308

E-mail: {sjurado, fgarijo, jss}@tid.es

1. Introduction

End-users¹ have the legal right to control how personal data about him/her is collected, used, shared and stored in any place. Apart from regulation reasons, end-users require such a protection as a means to become aware of the personal information given away and to increase their security, trust and convenience. That is, privacy protection of end-user personal data should involve not only regulatory requirements but also end-user preferences and permissions. Providing the end-user with this privacy protection will help an operator to establish a trust framework with customers, where the commercial relationship will take place.

On the other hand, operators are currently trying to position themselves in the services arena not only by directly offering end-user services but also by providing network and service capabilities to third party service providers (which in turn offer services to the operator customers). And all this has to be achieved considering end-users privacy restrictions, guaranteeing that his/her personal data are not shared with third parties without his/her consent.

Another important aspect is that end-users need to be provided with easy ways for defining his/her privacy preferences and permissions, being hidden the complexity of the process and considering as default policy a restrictive layout (for example, the default policy with regard to reception of advertisement messages should be “deny”, and only upon explicit request from the user, some service providers should be allowed to send him/her such messages).

In all corporations, and an operator is not an exception, there is the necessity of defining privacy policies that must be enforced when external access from other companies or end-users are involved. Therefore privacy should be guaranteed both in B2C and B2B environments. This consideration is fundamental when it comes to a telco operator, which has to consider not only the privacy protection of their employees but also and especially that of their customers. So that privacy languages should allow customers the definition of privacy preferences and restrictions that apply to his/her data. Such preferences and restrictions will be applied when other business entities (suppliers and other third parties) attempt to access customers' data. At the end, the process will have defined who is who and who is responsible for what. That is, it will have allowed to define with what organisations, companies, profiles, end-users, etc. an

¹ In this paper end-user refers to any possible telco operator customer, so it can be a single person, a company, an organisation, etc.

entity wants and needs to share information, what information and with what restrictions (an example of a possible type of restrictions are those related to DRM).

If we have a look at the existing technical approaches and solutions for all the questions described previously in this section, we can find two existing initiatives: XACML and P3P (with its language APPEL).

One of them, P3P, seems to be a good solution to define the end-user's privacy restrictions that should be applied to the user's personal information that the operator stores and manages, and therefore it is useful to build trust between the operator and its customers. But an approach as P3P will succeed, and hence be applicable, only if its adopted by the most popular navigators and websites. On the other hand, P3P is limited to the B2C world and does not allow the user to utilize different types of terminals and user agents (web browsers, mobile terminals, etc.), so that it does not seem to offer a complete solution for a telco operator.

In B2B, when third parties (other service providers) are involved, the decision of allowing or denying third parties to access end-users data should take into account the purpose of the request and the intended usage of the data. In this case, it is necessary the integration with other related standards, as those defined in the identity management arena, to provide an overall and integrated solution. Therefore, the combination of SAML and the XACML seems to be a good initiative.

2. Privacy languages requirements

In this section we will describe the main requirements that privacy languages and architectures must meet from a telco operator point of view.

Need of a complete framework: Although some standardization bodies have defined privacy solutions for particular services (for example 3GPP has defined a privacy solution for location based services), for a telco operator issues as time to market and OPEX and CAPEX optimisation are critical nowadays. Therefore, **languages and solutions for privacy management should apply in a common way to all resources** (services for example) and should be technology independent. In that sense, it is worthy to mention that privacy languages must integrate in an overall framework that guarantees users privacy.

Standards are desirable: Some vendors might be considering the option of adopting a standard or developing a proprietary privacy language. One of the advantages of standard languages is that enable the automation of the management of the privacy policies life cycle. It also eases the procurement process and simplifies the integration tasks. Hence, for an operator, **a standard adopted by all vendors is desirable** and means a great advantage. There are already some initiatives for defining a standard language based on XML: XACML, APPEL, EPAL, BPEL, IETF Common Policy, etc. But up to now none of these initiatives seems to have succeeded in defining a simple but general language re-usable in different contexts and largely adopted by the market and standardization bodies. And thought using XML as the underlying technology simplifies the integration task, there are performance penalties due to its text format that should be minimised.

Privacy ontology: An ontological framework will help modelling privacy concepts in order to look deeply into the understanding of privacy issues. Defining **a global privacy vocabulary understandable by all the entities involved in a privacy scenario** will be very helpful to assure that the privacy policy and its rules are applied as the entity that originated the privacy restrictions intended to. Therefore working on a privacy ontology that could become a standard largely adopted, is also something desirable.

Need to cope with convergent scenarios: Telco operators such as Telefónica have become convergent operators, meaning that they provide services to users over different technologies and terminals (fixed-line, mobile, etc.). Therefore, privacy solutions shall be able to cope with **different types of accesses, possibly using different types of terminals, networking technologies and user agents** (web browsers, mobile terminals, proprietary applications, web services, etc.).

Need to cope with service-oriented ecosystems where **multiple service providers** cooperate to provide dynamically end-user services and where individual privacy specifications must be guaranteed. This will require the real-time validation of individual privacy specifications versus permissions and obligations of the possible service providers, in order to select the most suitable.

Integration with legacy systems: Unfortunately, telco operators have been handling user private attributes and providing messaging services for a while. Thus, there are already privacy solutions operating in an operator such as Telefónica. Integration of the privacy languages and solutions defined with the existing legacy systems is a critical issue.

Performance is again a critical issue for any service provider, and a telco operator is not an exception. Privacy languages should take this matter into account, especially considering that most of the standards on privacy languages being defined nowadays (XACML, APPEL, etc.) are XML-based, which usually implies an overhead regarding processing time and memory. Therefore, when defining a privacy language, optimisation of traffic and resources consumption issues should be thought about.

SLAs support: SLA is a common way for establishing business contracts between two parts (an end-user and a company, between two companies, etc.). In the telco operator world, typical relationships are between the operator and third-party service providers. Definition of languages for the automation of SLA handling should support the establishment of privacy restrictions when it comes to accessing and processing user data.

Distributed privacy policies: Nowadays it is very common to have data distributed throughout several sources and repositories, and this can happen with data related to privacy restrictions. Therefore another requirement for a privacy language should be the **flexibility to storage the rules that define the privacy policies in a distributed way**. And, of course, allow access to those rules and policies from any place.

Other important aspects related to the definition of privacy policies that a privacy language should consider are:

- The possibility of defining **privacy policy profiles** and defining policies that **apply to a particular resource (service), to a group of resources or to all the resources**.
- Existence of a **rule-combining algorithm** to create a policy and of **complex structures** of privacy policy definition (for example one policy could refer to another).
- **Prioritising** the policies and rules that define a policy.
- Allowance for establishing **obligations**, and not only denials and authorisations, which provide liberty and flexibility to sort out conflicts resolution (for example providing for the possibility of contacting the end-user "on the fly", but of course avoiding asking repeatedly the user's consent which implies the storage of privacy restrictions).
- Parents are becoming increasingly concerned about what information do their children get and provide in the Internet, as the residential sector is a significant

percentage of an operator's customers their needs should be considered. Hence, **a hierarchical approach for privacy policies definition** should be provided.

- We live in a world of constant change, and some times those changes take place quicker than we would like. Hence, **privacy language policy attributes should be wide and allow easy extension** to provide two critical aspects flexibility and scalability.
- Finally, not only definition of privacy languages is desirable, but also **development of tools** that help managing and applying those languages and the administration (creation, validation and management) of the privacy preferences for different services, in several business and usage contexts. So this issue should be taken into account in the industrialisation process.

3. Use cases

In this section a brief description is given about some use cases where a privacy language and solution are the answer to the formulated difficulty.

Access to end-user location: The end-user's location information is very useful to provide several services (nearest points of interests as shops or restaurants, direction guides, workforce management, fleet management, etc.). An operator has access to this information, but not all end-users agree with the usage of this personal data by the operator or a third party, as they will probably consider it intrusive. Some end-users agree with the usage of this personal information but not for all the services that could be provided, for example they will approve giving away his/her location but only for services requested by him/her but not for advertising purposes or they will approve the usage of his/her location by the operator but not by third parties.

Parental control: In the previous section it was mentioned the fact that as the Internet and mobile phones become more popular, parents are becoming concerned about what information do their children get from the Internet and give away, what kind of calls do they get or do they make, etc. Parents need to be provided with the ability to define the privacy policies that should be applied to their children, avoiding access to a particular service or types of services (for example for adults). And limiting the preferences that their children can establish, for example if parents have purchased a service that gives information about the location of their children by means of their mobile phone, then children can not define in their privacy preferences that they do not agree with the usage of his/her location information.

Spam prevention: Spam is a problem that is getting worse every day, not only because of the amount of undesirable mails, messages or even calls you get, but also because some of those messages or calls hide bad intentions. In order to sort out this problem, end-users should have the possibility of defining privacy policies that can help filtering and therefore avoiding that undesired content.

4. Conclusions

End-users are concerned about security and protection of their personal information, so privacy safety of this information should go beyond regulatory requirements allowing end-users define and manage their own preferences and permissions. Operators and service providers need to establish a trust framework which facilitates the specification and validation of customer's permissions, and guaranties privacy protection both in B2C and B2B environments. This guarantee will provide the telco operator with the means for supplying a trusted services offer.

In order to successfully provide such service offer, the telco operator needs to meet some fundamental requirements on privacy languages and architectures. Those

requirements are **need of a complete framework** technology independent, and based on standards. Privacy languages are part of such complete framework. **Need to cope with convergent scenarios and with service oriented ecosystems** where multiple service providers cooperate to provide dynamically end user services. **Integration with legacy systems, performance, privacy ontology, SLA support and distributed privacy policies** seem also key requirements that should be complemented by the **development of supporting tools** which will facilitate managing and applying privacy languages and the administration of the privacy preferences.

A standardised, largely adopted and complete framework is crucial for a convergent operator, in order to help minimising time to market and for the optimisation of CAPEX and OPEX.

The bases are already established, thanks to the achievements on the identity management field and initiatives as XACML and P3P. However, there is still a lot of effort to be done to meet the requirements identified. Closer cooperation between the industry, the academic world and standardisation bodies should continue to advance towards technical solutions that satisfy customers, businesses and technical needs.

5. References

- [1] [OASIS eXtensible Access Control Markup Language \(XACML\) TC](#)
- [2] [W3C P3P Project Main Page](#)
- [3] [A P3P Preference Exchange Language 1.0 \(APPEL1.0\)](#)
- [4] [OASIS Security Services \(SAML\) TC](#)
- [5] [Enterprise Privacy Authorization Language \(EPAL\)](#)
- [6] [Business Process Execution Language for Web Services version 1.1](#)
- [7] [Liberty Alliance Project](#)