Privacy Token: An Improved and Verified Mechanism for User's Privacy Specification in Identity Management Systems for the Cloud

María Elena Villarreal, Sergio Roberto Villarreal, Carla Merkle Westphall, and Jorge Werner

Network and Management Laboratory
Post-Graduate Program in Computer Science
Federal University of Santa Catarina
Florianopolis, SC, Brazil
Email: maria.villarreal@posgrad.ufsc.br, sergio@lrg.ufsc.br,
carla.merkle.westphall@ufsc.br, jorge@lrg.ufsc.br

***Abstract*— With the increasing amount of personal data stored and processed in the cloud, economic and social incentives to collect and aggregate such data have emerged. Therefore, secondary use of data, including sharing with third parties, has become a common practice among service providers and may lead to privacy breaches and cause damage to users since it involves using information in a non-consensual and possibly unwanted manner. Despite numerous works regarding privacy in cloud environments, users are still unable to control how their personal information can be used, by whom and for which purposes. This paper presents a mechanism for identity management systems that instructs users about the possible uses of their personal data by service providers, allows them to set their privacy preferences and sends these preferences to the service provider along with their identification data in a standardized, machine-readable structure, called privacy token. This approach is based on a three-dimensional classification of the possible secondary uses of data, four predefined privacy profiles and a customizable one, and a secure token for transmitting the privacy preferences. The applicability and the utility of the proposal were demonstrated through a case study, and the technical viability and the correct operation of the mechanism were verified through a prototype developed in Java in order to be incorporated, in future work, to an implementation of the OpenID Connect protocol. The main contributions of this work are the preference specification model and the privacy token, which invert the current scenario where users are forced to accept the policies defined by service providers by allowing the former to express their privacy preferences and requesting the latter to align their actions.**

Keywords–Privacy; Cloud Computing; Identity Management.

I. INTRODUCTION

This paper extends [1], which proposes a mechanism for users to control the secondary use of their Personally Identifiable Information (PII) based on a model to classify and represent privacy preferences and a secured token, called privacy token, by enhancing the model, and presenting a case study and an improved and more comprehensive prototype.

Cloud Computing offers infrastructure, development platform and applications as a service, on demand and charged according to usage. On the one hand, this paradigm gives users greater flexibility, performance and scalability without the need to maintain and manage their own IT infrastructure. On the other hand, it aggravates the problem of application and verification of security and causes users to lose, at least partially, control over their data and applications [2].

With the increasing amount of personal data stored and processed in the cloud, including users' Personally Identifiable Information (PII), economic and social incentives to collect and aggregate such data have emerged. Consequently, secondary use of data, including sharing with third parties, has become a common practice among Service Providers (SPs) [3]. However, since users only interact directly with SPs, which do not provide clear policies to warn them about how their PII can be used, they are usually unaware of secondary use of data and the existence of third parties [4].

According to the privacy taxonomy defined in [5], secondary use consists in the use of data for purposes other than those for which they were initially collected without the consent of the subject, e.g., the use of personal data collected on social networks for offering personalized advertising. This practice, thus, may violate the privacy of the user and cause damage since it involves using information in a non-consensual and possibly unwanted manner [5]. Nonetheless, whether certain action violates the privacy of a user depends on the perception of such user and his or her willingness to share given types of data. This, therefore, raises the need of collecting and respecting the privacy preferences of users.

An important aspect of the implementation of privacy in the cloud is Identity Management (IdM), which allows Identity Providers (IdPs) to centralize user's identification data and send it to SPs in order to enable the processes of authentication and access control [6]. IdM systems, such as OpenId Connect [7] and Shibboleth [8], allow the creation of federations, i.e., trust relationships that make possible for users authenticated in one IdP to access services provided by various SPs belonging to different administrative domains. An example is when users authenticate in different services with their Facebook accounts. In this case, Facebook acts as an IdP.

Even though there are several approaches that are intended to allow users to define their privacy preferences and organizations to express their practices, they are poorly adopted by both users and companies because they do not offer practical methods. In addition, most of them do not consider the decentralized nature of federated cloud environments. Consequently, IdM systems do not offer effective mechanisms to collect user's privacy preferences and to send them to the SP and, therefore, users are still unable to control how their PII can be used, by whom and for what purposes [2].

Werner and Westphall [9] proposed a privacy-aware identity management model for the cloud in which IdPs and SPs interact in dynamic federated environments to manage identities and ensure user's privacy. The model, while allowing users to choose and encrypt the data that can be sent to the SP, does not define a mechanism for determining users' privacy preferences and allowing them to control the use and sharing of their PII.

In order to complement the aforementioned model, this paper presents a mechanism for identity management systems that instructs users about the possible uses of their personal data by service providers and allows them to set their privacy preferences. These preferences are converted into a standardized, machine-readable structure, called privacy token, which is then sent to the SP along with other authentication data.

The remainder of this paper is organized as follows. Section II describes basic concepts relevant to the understanding of the proposal and Section III presents the main related work. In Section IV, the privacy mechanism is proposed. In Section V, a case study is presented, and, in Section VI, a prototype implementation of the mechanism is described. Finally, conclusion and future work are presented in Section VII.

II. Basic Concepts

This section presents the definitions of concepts considered important to the understanding of the proposal of this paper.

A. Identity Management (IdM)

IdM is implemented through IdM systems such as OpenId Connect [7], and is responsible for establishing the identity of a user or system (authentication), for managing access to services by that user (access control), and for maintaining user identity profiles [10].

Typical identity management systems involve three parts: users, identity providers, and service providers [10]. The user visits an SP, which, in turn, relies on the IdP to provide authentic information about the user. These systems enable the concept of federated identity, which is the focus of this work and allows users authenticated in various IdPs to access services offered by SPs located in different administrative domains due to a previously established trust relationship [11].

Some important IdM concepts are described next, as defined in [6][12][13]:

1) Personally Identifiable Information (PII): information that can be used to identify the person to whom it relates or can be directly or indirectly linked to that person. Thus, depending on the scope, information such as date of birth, GPS location, IP address and personal interests inferred by the tracking of the use of web sites may be considered as PII.

2) PII Principal: natural person to whom the PII relates.

3) Identity: computational representation of an entity active in a system, such as a person, a network device, or a programming agent.

4) Resource: entity, such as an application or a file, to which a user requires access.

5) Identity Provider (IdP): party that provides identities to subjects and is, usually, responsible for the process of authentication.

6) Service Provider (SP): party that provides services or resource access to users and, for that, requires the submission of valid credentials.

B. Privacy

Westin [14] defines privacy as the right of individuals, groups or institutions to determine for themselves when, how, and what information about them can be revealed to others.

According to the author, an essential aspect of human beings' freedom involves control over their personal information. Thus, his definition of privacy highlights the ability of people to decide on the amount, recipients, and conditions for disclosure of their personal data.

In this work, which focuses on IdM systems and federated cloud environments, privacy is considered to be the right of a user to decide if his or her PII can be used, by whom and for what purpose [5][13][15].

1) Privacy policy: set of statements that express the practices of the organizations regarding user data collection, use, and sharing.

2) Privacy preferences: preferences and permissions of a user for the secondary use of his or her PII, i.e., they determine by whom and for what purpose a PII can be used.

One way to achieve privacy in computer systems is through the implementation of Privacy Enhancing Technologies (PETs). According to ISO/IEC 2011 [13], PETs are privacy controls that consist of Information Technology measures, products or services that protect users' privacy by eliminating or reducing PII, or by preventing processing of unnecessary or unwanted PII.

III. Related Work

This section presents the work in which the proposal of this paper is based and other approaches that aim at providing privacy to users in computational environments.

A. Classification of Users by Privacy Preferences

Chanchary and Chiasson [16] performed an online survey to understand how users perceive online tracking for behavioral advertising. They demonstrated that users have clear preferences for which classes of information they would like to disclose online and that some would be more prone to share data if they were given prior control of tracking protection tools. The authors also identified three groups of users according to how their privacy attitudes influenced their sharing willingness. These groups are used as a basis for the privacy profiles of our mechanism and are presented next:

1) Privacy Fundamentalists (30.4%): consider privacy as a very important aspect and they feel very strongly about it.

2) Privacy Pragmatists (45.9%): consider privacy as a very important aspect but also like the benefits of abdicating some privacy when they believe their information will not be misused.

3) Privacy Unconcerned (23.6%): do not consider privacy an important aspect or do not worry about how people and organizations use their information.

B. Privacy Policy Languages

Platform for Privacy Preferences (P3P) [17] is a protocol designed to inform users about the practices of collecting and using data from websites. A P3P policy consists of a set of eXtensible Markup Language (XML) statements applied to specific resources such as pages, images, or cookies. When a website that has its policies defined in P3P wants to collect user's data, the preferences of that user are compared to the corresponding policy. If this is acceptable, the transaction continues automatically; if not, the user is notified and can opt-in (accept) or opt-out (reject). This work provides a basis for collecting user preferences, but it requires every user and SP to define their policies in this language and does not meet the needs of federated cloud environments.

Enterprise Privacy Authorization Language (EPAL) [18] is a formal language designed to address the industry's need to express organizations' internal privacy policies. An EPAL policy defines a list of hierarchies of data categories, user categories and purposes, as well as sets of actions, obligations, and conditions. These elements are used to formulate privacy authorization rules that allow or reject actions. Nevertheless, as it is specific for internal corporate policies, it does not consider user's preferences and is not suitable for privacy in federated identity environments.

Purpose-to-Use (P2U) [3] was proposed to provide means to define policies regarding the secondary use of the data. It is inspired by P3P, but allows the specification of privacy policies that define the purpose of use, type, retention period, and price of shared data. This language, although it enables user-editable and negotiable policies, is complex for users as it assumes that they have privacy policies and are able to define them in P2U. It also requires the SPs to have their policies defined in the same language.

C. UML Privacy Profiles

Basso et al. [19] define a Unified Modeling Language (UML) profile to assist in the development of applications and services that need to be consistent with the statements of their privacy policies. The authors identify privacy elements, such as policies and statements, through which organizations can define their policies for collecting, using, retaining, and releasing data; and organize their relationships into a conceptual model. This model is then mapped to a UML profile defined by stereotypes, attributes, and constraints that allow modeling statements of actual privacy policies. Although this profile helps application developers, it does not offer practical means for users to set their privacy preferences and transmit them to SPs.

D. Privacy Mechanisms of IdM Systems

Two of the most widely adopted identity management systems for federated environments are Shibboleth and OpenID Connect. Both IdM systems have embedded privacy mechanisms, which are described next.

Shibboleth, until its second version, had an extension for the IdP and called uApprove that added a stream to obtain user consent for the release of their data. As of the third version, with Shibboleth design changes, the consent mechanism came to be provided as standard [8].

This mechanism requires users to accept the release of attributes for service providers during authentications that include attribute data in the response [8]. Thus, users are requested to give consent for the release of attributes:

- In the first access to the resources of an SP;
- When releasing an attribute for which consent was not given before;
- When an attribute for which consent has already been given is no longer released; and
- When the value of an attribute for which consent has already been given changes.

It is possible to enable consent by attribute to allow the user to select the attributes that she or he wants to release and to define lists of attributes to which the user must always be asked to consent (whitelist), attributes for which the user should not be prompted to consent (blacklist), and attributes corresponding to a regular expression to which the user should be asked to consent (Regex).

Regarding the duration of consent for data release, users can choose between three options: to be asked for each login, to be asked if the attributes provided for a given service have changed since consent was given (standard option), and never to be asked (optional). With the last option, called global consent, all attributes are released to any service provider.

Shibboleth's mechanism, however, has some limitations. For many services, for example, the list of attributes to which the user must give consent can be very extensive, which increases complexity and often leads users to release all data and choose not to be requested in following accesses. In addition, the requested permission is only for the release of data that will be explicitly sent to the service provider by the IdP to enable the service and, therefore, this mechanism does not consider the secondary uses of such data and does not include information that may be inferred by the SP, as well as it does not make users aware about possible secondary uses of their data.

OpenID Connect (OIDC), in turn, has an integrated privacy mechanism that allows users to consent or deny the release of certain types of data to the service provider [20].

The OIDC Authorization Server, after user authentication, must obtain authorization before releasing information to the SP. The latter uses scopes to specify which access privileges are requested for a given resource, and the user uses them to determine which specific sets of attributes are available to the service provider. An application can request the specific permissions it needs through the scope parameter.

OpenID Connect defines the following scopes of data:

- *openid*: this scope is required and informs the Authorization Server that the SP is making an OpenID Connect request;
- *profile*: this scope requests access to the default attributes of the user's profile, such as name, surname, username, photo, gender, and date of birth;
- *email*: this scope requests access to the attributes related to the user's email;
- *address*: this scope requests access to the address attribute;
- *phone*: this scope requests access to attributes related to the user's phone; and

- *offline_access*: this scope requests access to the user's UserInfo even when the user is not logged in.

As the mechanism present in Shibboleth, OpenID Connect only requests the user's authorization for the IdP to provide the data requested by the SP to offer the service and, therefore, does not include information that may be induced by the service provider and does not consider the possible secondary uses of data.

E. User-Centric Privacy Architecture

Kolter [4] proposes a user-centric and SP-independent privacy architecture. This architecture comprises a collaborative privacy community and three user-side privacy management components, which are explained next.

The Privacy Community allows users to exchange information about privacy, ratings, and experiences about service providers, such as the amount of personal information needed to fill out a form, and third parties with whom the SP shares information. The Privacy Preference Generator provides a tool for users to set their privacy preferences. The Privacy Agent, on the other hand, shows relevant information from the Privacy Community, the evaluation of the privacy policy, and the reputation given by the community to the visited website, and compares the preferences generated by the Privacy Preference Generator with machine-readable privacy policies. The Data Disclosure Log component, in turn, records personal data transfers and provides an overview of past personal data streams [4].

This architecture, however, is complex and not completely independent of the SP since it demands that providers express their policies in P3P. The Privacy Agent requires the user to install an extension on their browser; the Privacy Community demands users to maintain and provide reliable information and explanations of providers' privacy policies; and the Privacy Preference Generation tool requires users to define specific preferences for the twelve types of services offered by SPs and extensively lists the data divided into nine types. If a service type is not configured, the tool understands that the user does not want to interact or make available any personal data with SPs that offer this type of service.

F. Model for IdM with Privacy in the Cloud

Werner and Westphall [9] present an IdM model with privacy for the cloud in which IdPs and SPs interact in dynamic and federated environments to manage the identities and ensure the privacy of users. They propose predefined, customizable privacy settings that help users to declare their desired level of privacy by allowing them to choose the access model, which can be anonymous, pseudonymous, or with partial attributes, and warning them about the reputation of the SP.

The interaction model defined in [9] and shown in Figure 1 proposes the registration in the IdP of the user's attributes and credentials, which may be encrypted (step 1), as well as the privacy policies to regulate the use and dissemination of their PII (step 2). Both the data and the policies are encapsulated in a package called sticky policies, which is sent to the SP along with a data dissemination model and obligations that must be fulfilled by the SP. The idea of the sticky policies is that PII is always disseminated with the policies governing their use and dissemination so that the user's privacy preferences are met

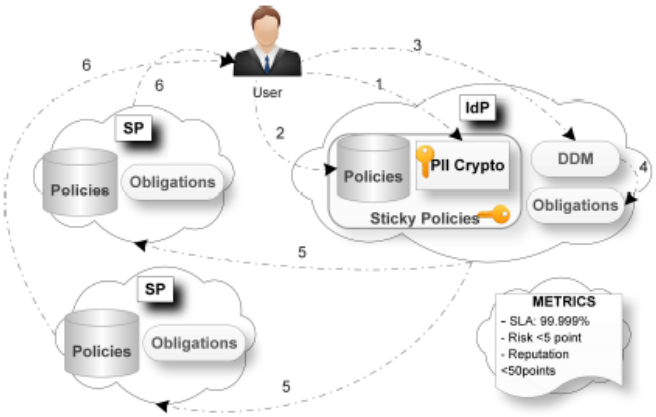

Figure 1. Interaction model between user, IdP and SP proposed in [9].

by any SP. If the policies of the SP and the sticky policies are compliant, a positive reputation assess is generated for the SP; otherwise, a low reputation score is returned. The authors, however, do not define a mechanism for collecting user's preferences, converting them into a machine-executable structure, and sending them to the SP.

IV. Proposal for a Privacy Preferences Specification Mechanism

This work aims at providing users with control over the secondary use of their PII and, consequently, protect them against the misuse of their data, through a model to classify and represent privacy preferences and a mechanism to implement such model [1].

The model consists of a comprehensive, three-dimensional classification of possible uses of PII that gives rise to a set of forty-five preferences, and four predefined privacy profiles based on these preferences.

The mechanism, in turn, enables users to select a predefined privacy profile or create a custom one. This profile is then transformed into a privacy token, a secure token similar to the ID and access tokens already used by the OpenID Connect protocol, and sent to the service provider.

A. Classification of Possible Uses of PII

Due to the large amount of possible actions and methods for collecting and sharing data, it is unfeasible to thoroughly list them. Therefore, this paper proposes a generic model that, on the one hand, is useful for users to set their privacy preferences and, on the other hand, works as a reference for SPs to assess whether the business rules of their data collection applications meet these preferences.

For this purpose, possible uses of the PII were classified in a three-dimensional structure. The dimensions, along with their respective abbreviations, are described next:

1) Data type: category of the PII to which the preference refers. The attributes of this dimension are:

- *Personal Identification (PI)*: encompasses any kind of information that represents the PII principal, such as name, national identifiers, email, cellphone number, and photo;

- *Personal Characteristics and Preferences (PCP)*: are considered to be the physical attributes of the PII principal and personal options like weight, religious or philosophical beliefs, and sexual orientation;
- *Location (LO)*: refers to any information about where the user is or has been and his or her trajectories with any precision degree and obtained by any means, such as GPS, Wi-fi networks or telecommunications systems;
- *Activities and Habits (AH)*: any activities performed by the user and habits inferred from tracking, such as web sites visited, purchases, and behavioral profile; and
- *Relationships (RS)*: people with whom the PII principal is in a specific moment or interacts through means like social networks, emails, and instant messengers.

2) Purpose: purpose for which the PII can be used. The values of this dimension are:

- *Service Improvement (SI)*: refers to the use of data for implementing improvements in the services offered, such as customization of functionalities, greater usability, and increased security;
- *Scientific (SC)*: concerns the granting of data for academic and scientific research; and
- *Commercial (CO)*: represents the use of user's PII to develop or offer new products and services with the purpose of obtaining commercial benefits.

3) Beneficiary: party that benefits with the use of the PII. The attributes are:

- *PII Principal (PP)*: corresponds to the user who accesses the service and to whom the PII is related;
- *Service Provider (SP)*: refers to the party responsible for offering the services accessed by users and for processing their data; and
- *Third Party (TP)*: represents a party interested in the data different and independent from the PII Principal and the service provider.

The dimensions above define a structure in which each position represents a rule that expresses a user's privacy preference that must be respected by the SP. This way, each of these rules comprises three parts: the type of data the rule refers to, for what purpose it can be used, and for the benefit of whom it can be used. For example, a user can define that his or her location data can be used for the purpose of improving services for the benefit of the PII principal and, in another rule, define that the same type of information for the same purpose cannot be used for the benefit of a third party.

By using the presented classification, the user's privacy preferences can be collected in a detailed manner or through four predefined profiles, which are described in the next section.

B. User's Privacy Profiles

Through the classification presented in the previous subsection, the user's privacy preferences can be collected individually or through four predefined profiles. These profiles were defined based on the work in [16], presented in Section III, which classifies users into three groups according to their privacy concerns. Given that the *Privacy Pragmatist* group has the highest percentage of users and in order to offer more representative options, it has been subdivided into *Privacy Aware* and *Privacy Pragmatist*.

Table I. Configuration of the preferences of each predefined privacy profile regarding the secondary uses of PII.

PREFERENCES			PROFILES			
Data Type	Purpose	Beneficiary	F	A	P	U
Personal Identification (PI)	Service Improvement	PII Principal		✓	✓	✓
		SP			✓	✓
		Third Party				✓
	Scientific	PII Principal		✓	✓	✓
		SP		✓	✓	✓
		Third Party		✓	✓	✓
	Commercial	PII Principal		✓	✓	✓
		SP			✓	✓
		Third Party				✓
Personal Characteristics and Preferences (PCP)	Service Improvement	PII Principal		✓	✓	✓
		SP			✓	✓
		Third Party				✓
	Scientific	PII Principal		✓	✓	✓
		SP		✓	✓	✓
		Third Party		✓	✓	✓
	Commercial	PII Principal			✓	✓
		SP				✓
		Third Party				✓
Location (LO)	Service Improvement	PII Principal			✓	✓
		SP				✓
		Third Party				✓
	Scientific	PII Principal			✓	✓
		SP			✓	✓
		Third Party			✓	✓
	Commercial	PII Principal			✓	✓
		SP			✓	✓
		Third Party				✓
Activities and Habits (AH)	Service Improvement	PII Principal		✓	✓	✓
		SP		✓	✓	✓
		Third Party			✓	✓
	Scientific	PII Principal		✓	✓	✓
		SP		✓	✓	✓
		Third Party		✓	✓	✓
	Commercial	PII Principal		✓	✓	✓
		SP			✓	✓
		Third Party			✓	✓
Relationships (RS)	Service Improvement	PII Principal		✓	✓	✓
		SP		✓	✓	✓
		Third Party			✓	✓
	Scientific	PII Principal		✓	✓	✓
		SP		✓	✓	✓
		Third Party		✓	✓	✓
	Commercial	PII Principal			✓	✓
		SP			✓	✓
		Third Party				✓

The four predefined profiles are described in the following paragraphs and the values of the privacy preferences for each of them are shown in Table I. In this table, the privacy profiles are represented by their initials and each row corresponds to a preference regarding the use of a type of data for a particular purpose and for the benefit of a specific part. Thus, preferences checked with a "✓" represent the user's consent to the use of the data.

1) Privacy Fundamentalist: This profile is aimed at users who have very high concerns with their privacy and do not wish their data to be used for any purpose other than the one for which they were collected. Some features, however, may not work properly or at all when this profile is chosen. In addition, any opportunities for service improvements and personalized offers of products and services will be missed.

2) Privacy Aware: This profile represents users who are concerned about their privacy but still want to enable most functionalities and service improvements, and receive some opportunities of personalized offers of products and services without sharing data with third parties.

3) Privacy Pragmatist: This profile is aimed at users who still want some privacy but also want to enable all the functionalities and service improvements. These users allow a restricted sharing of data with third parties in order to enable several personalized offers of products and services.

4) Privacy Unconcerned: This profile is for users who are not concerned about their privacy or how their PII is used, hence any data can be disclosed for any purpose and in the benefit of anyone according only to the privacy policy of each SP. All services and personalized offers of products and services are enabled with this profile.

Beside simplifying the process of setting the privacy preferences, these profiles are clarifying for the users as they inform about the possible uses of their PII and levels of risks to privacy, and, as a result, assist them in making a conscious decision. In addition, users have the possibility to customize their privacy preferences using any of the profiles above as a basis.

C. Privacy token

Once the profile is chosen or customized, the privacy preferences, along with additional information, are converted into a JSON (JavaScript Object Notation) object, which is then used as the payload for creating a JSON Web Token (JWT) signed or protected with Hash-based Message Authentication code (HMAC), and encrypted. The final object is called privacy token and is generated by the IdP and sent to the SP, which must validate it in order to verify its integrity and use its information to guide the behavior of their data usage applications.

The structure of the privacy token, illustrated in Figure 2, comprises three sections. The first one is the header, which declares that the data structure is a JWT and defines the security algorithm chosen and implemented by the IdP (in this example, SHA-256); the second section consists of the claims set, which is explained next; and the last section contains the signature of the token.

The claims set includes two parts. The first one defines the following claims inherited from the ID token: *sub*, which is the subject identifier, i.e., a sequence of characters that uniquely identifies the PII principal; *iss*, which identifies the authority issuing the token, i.e., the IdP; *aud*, which represents the intended audience, i.e., the SP; and *iat*, which declares the time at which the token was issued.

The second part of the claims set define the privacy preferences of the user. Each claim corresponds to a position of the structure presented in Section IV-A, i.e., a privacy preference, and has a boolean value. The structure of a claim is as follows: the first abbreviation represents the type of data, the second abbreviation refers to the purpose, and the last one represents the beneficiary. For example, if the value of the attribute *LO_CO_SP* is true, it means that location data can be used for commercial purpose in the benefit of the SP.

To ensure its integrity, the privacy token must be protected through an HMAC or a digital signature and then encrypted in order to protect its content and maintain its confidentiality as well as hinder its tampering. The encryption can be symmetric or asymmetric according to the choice and implementation of each identity provider. The use of digital signature or HMAC also depends on the choice of the IdP, which is responsible for sharing the secret key in the second case.

Figure 2. Structure of the privacy token.

The token is secured through the Sign-then-Encrypt method to prevent attacks where the signature is removed by leaving only an encrypted message, provide privacy to the signer, and ensure that the signature is always accepted, since signatures on encrypted text are not valid in some jurisdictions.

Once signed and encrypted, the privacy token is sent to the SP via the user's browser. To perform this transmission efficiently and without compromising the system's performance, the token is encoded in a Base64 string, which can be embedded in a Uniform Resource Locator (URL). After receiving the token, the SP must send it back to the IdP and request its validation. The latter, after verifying the integrity of the privacy token, sends a validity confirmation to the service provider.

The privacy token must always be passed along with the ID token, for instance, when the ID token has expired and a new one is requested to the IdP, when passing identity to third parties or when exchanging the ID token for an access token. This is necessary to ensure that users' PII is always accompanied by the corresponding privacy preferences. This way, with the addition of the privacy token, the OpenId Connect modified flow presented in [9] would be extended, as shown in Figure 3, to encompass the following steps:

1) The user requests access to a resource in the SP;
2) The security manager at the SP asks for the user to authenticate in the IdP where she or he is registered;
3) The IdP asks for the user's credentials;
4) The user provides his or her credentials;
5) The IdP validates user's credentials and returns the ID token and the privacy token to the user, who passes it to the SP;

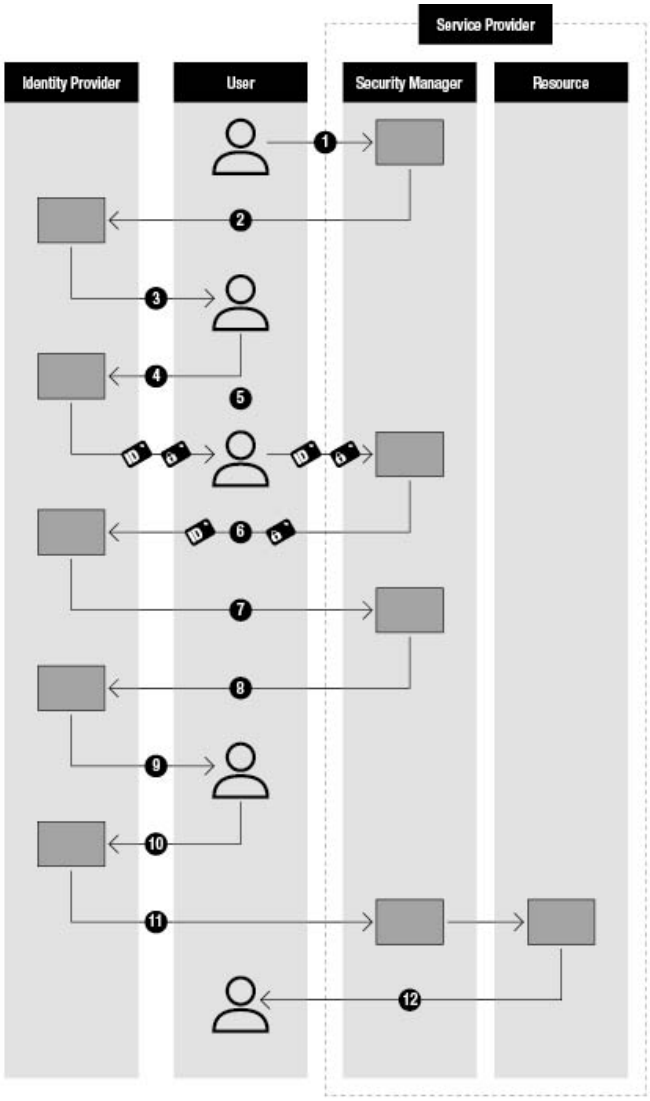

Figure 3. Extension of the IdM flow proposed in [9] with the addition of the privacy token.

6) The SP sends the ID and the privacy tokens to the IdP for the proof of validation;
7) The IdP verifies the tokens and confirms their validity to the SP;
8) The SP requests additional attributes to the IdP;
9) The IdP shows the data dissemination scopes supported by the SP for the user to choose;
10) The user chooses one of the scopes, and informs the IdP about the selected scope;
11) The IdP provides the data to the SP according to the selected scope;
12) The SP allows the user to access the desired resource.

The privacy profile that is used for generating the privacy token sent to the SP in Step 5 is chosen or customized by the user during the process of registration in the IdP. In order to offer more flexibility, users can change their choice at any moment requesting it to the IdP.

V. Case Study

To demonstrate the applicability, utility and potential of the proposed model, it was applied in a hypothetical case of an online event registration service. This example shows how, despite the simplicity of the service and the small amount of data provided directly by the user, there is a great potential for secondary uses of this data, and also how the application of the model can limit the abuses by the service provider and the invasion of user's privacy.

The case analyzed consists of a service provider that offers an online event registration service. To do so, the organizers register their events and the SP provides the users with an online page with information about the event and means for registering and paying. In order to use this service, the user must be registered in an IdP belonging to the same federation as the service provider and must authenticate in the SP through this IdP. Besides, it may be necessary to provide additional data to the service provider, which keeps a record of subscriptions made by users to facilitate registration in future events.

In this case study, a street race is used as example and the SP requests the following data to the organizer of the event to register it:

- Name of the organizer;
- National identifier;
- Name of the person in charge;
- Official name of the event;
- Type of race;
- Categories;
- Location of the race;
- Date and time of the event; and
- Price of registration.

To allow the user to use the system, the service provider requires the following data, which can be obtained directly by the IdP or explicitly requested to the user:

- Full name;
- Date of birth;
- Gender;
- National identifier; and
- Email.

In order to register for the race, the user is requested to provide the following additional data to the SP:

- Cellphone number;
- Height;
- Weight;
- Distance to be run; and
- Payment data.

In addition to the data supplied by the user, the SP may collect context data at the time of the registration, such as:

- Location;
- Time of the registration;
- Device used;
- Type of connection; and

- Group of people who registered from the same device and at the same moment.

Based on the data provided and collected in the registration, on the user's registration history, and on other registrations made in the event, it is also possible to infer further information, such as:

- Time when the user usually registers for races;
- Devices and types of technology most used to make the registrations;
- Group of people who paid with the same credit card;
- Group of people who will participate together of the event (registrations made in the same context);
- Members of a family;
- Whether the user participates in races with family members;
- Frequency of user's participation in races;
- Categories preferred by the user;
- Level of physical conditioning of the user;
- User's habits of participating in outdoor activities;
- Place where the registered user will be on the date of the event;
- People who will be together at the venue on the day of the event;
- User's usual payment method;
- User's credit card brand;
- Whether the user has more than one credit card;

Finally, the collected data can be aggregated to data from other events for which the user has registered and from other sources to infer new information.

A. Possible Secondary Uses of Data

From both collected data and inferred information, a great number of possible secondary uses arise, some of which, defined based on actual privacy policies, are presented next classified according to the type of the data.

For the Personal Identification type of data, the following possible secondary uses have been defined:

- Add name and email to a list of notifications about the event in which the user has registered;
- Add name and email to mailing lists of the SP to promote new events;
- Add name and email to a list of valid emails to be sold to third parties; and
- Store national identifier, name, and cell phone of the participant in the database of the SP to facilitate registration in upcoming events.

The possible secondary uses defined for the Personal Characteristics and Preferences type of data are:

- Add national identifier and age to a list to be conceded to a university research project to compile statistics of participation in races by age;
- Add name and email of people who have more than one credit card to a list to be sold for advertising a real estate project;
- Add email and age to a list of people to be sold to a company that sells food supplements;
- Add email, height, and weight to a list of men and women who weigh more than certain amounts to be offered to plus-size stores; and
- Store national identifier, gender, and age of the participant in the database of the SP to facilitate registration in upcoming events.

For the Location type of data, the following possible secondary uses have been defined:

- If the registration is made from a mobile device, provide cell phone number and location to a company that specializes in offering advertising services based on location;
- Use the location of the user at the time of registration to offer tickets to other events near such location;
- When the distance between the location of the user at the time of registration and the location of the event is greater than a certain amount, offer transportation and lodging services;
- Use the location of the event to offer tickets to other events near such location; and
- Add name and email of the participant and date of the event to a list to be sold to restaurants near the location of the race.

The possible secondary uses defined for the Activities and Habits type of data are:

- Use data about the usual form of payment for automatically filling the registration form;
- Add email and preferred types of races to lists to be sold to companies that sell sporting goods; and
- If the user travels frequently to participate in events, add email and participation frequency in events to a list to be sold to home security companies.

For the Relationship type of data, the following possible secondary uses have been defined:

- Add email and family group to a list to be provided to a Ministry of Health research project about people participating in races with family; and
- Offer a collective vehicle rental to people who have registered in the same context.

B. Application of the Model

This subsection shows how the application of the model and the choice of the profile by users modify and restrict the behavior of the SP regarding the use of their data. Each case describes how the data usage application of the service provider acts according to the predefined privacy profile chosen by the user.

1) Case 0: No Application of the Model: If the model is not used, the SP may perform all the secondary uses aforementioned without the knowledge or the consent of the user. These uses are only conditioned by the privacy policies of the service provider, when they exist.

Table II. Possible secondary uses allowed and not allowed with the Privacy Aware profile.

PRIVACY AWARE PROFILE	
ALLOWED SECONDARY USES	PREFERENCE
Add name and email to a list of notifications about the event in which the user has registered.	PI_SI_PP
Store national identifier, name, and cell phone of the participant in the database of the SP to facilitate registration in upcoming events.	PI_SI_PP
Add national identifier and age to a list to be conceded to a university research project to compile statistics of participation in races by age.	PCP_SC_TP
Store national identifier, gender, and age of the participant in the database of the SP to facilitate registration in upcoming events.	PCP_SI_PP
Use data about the usual form of payment for automatically filling the registration form.	AH_SI_PP
Add email and family group to a list to be provided to a Ministry of Health research project about people participating in races with family.	RS_SC_TP
SECONDARY USES NOT ALLOWED	PREFERENCE
Add name and email to mailing lists of the SP to promote new events	PI_CO_SP
Add name and email to a list of valid emails to be sold to third parties.	PI_CO_TP
Add name and email of people who have more than one credit card to a list to be sold for advertising a real estate project.	PCP_CO_TP
Add email and age to a list of people to be sold to a company that sells food supplements.	PCP_CO_TP
Add email, height, and weight to a list of men and women who weigh more than certain amounts to be offered to plus-size stores.	PCP_CO_TP
If the registration is made from a mobile device, provide cell phone number and location to a company that specializes in offering advertising services based on location.	LO_CO_TP
Use the location of the user at the time of registration to offer tickets to other events near such location.	LO_CO_SP
When the distance between the location of the user at the time of registration and the location of the event is greater than a certain amount, offer transportation and lodging services.	LO_CO_SP
Use the location of the event to offer tickets to other events near such location.	LO_CO_SP
Add name and email of the participant and date of the event to a list to be sold to restaurants near the location of the race.	LO_CO_TP
Add email and preferred types of races to lists to be sold to companies that sell sporting goods.	AH_CO_TP
If the user travels frequently to participate in events, add email and participation frequency in events to a list to be sold to home security companies.	AH_CO_TP
Offer a collective vehicle rental to people who have registered in the same context.	RS_CO_SP

Table III. Possible secondary uses allowed and not allowed with the Privacy Pragmatist profile.

PRIVACY PRAGMATIST PROFILE	
ALLOWED SECONDARY USES	PREFERENCE
Add name and email to a list of notifications about the event in which the user has registered.	PI_SI_PP
Add name and email to mailing lists of the SP to promote new events	PI_CO_SP
Store national identifier, name, and cell phone of the participant in the database of the SP to facilitate registration in upcoming events.	PI_SI_PP
Add national identifier and age to a list to be conceded to a university research project to compile statistics of participation in races by age.	PCP_SC_TP
Store national identifier, gender, and age of the participant in the database of the SP to facilitate registration in upcoming events.	PCP_SI_PP
Use the location of the user at the time of registration to offer tickets to other events near such location.	LO_CO_SP
When the distance between the location of the user at the time of registration and the location of the event is greater than a certain amount, offer transportation and lodging services.	LO_CO_SP
Use the location of the event to offer tickets to other events near such location.	LO_CO_SP
Use data about the usual form of payment for automatically filling the registration form.	AH_SI_PP
Add email and preferred types of races to lists to be sold to companies that sell sporting goods.	AH_CO_TP
If the user travels frequently to participate in events, add email and participation frequency in events to a list to be sold to home security companies.	AH_CO_TP
Add email and family group to a list to be provided to a Ministry of Health research project about people participating in races with family.	RS_SC_TP
Offer a collective vehicle rental to people who have registered in the same context.	RS_CO_SP
SECONDARY USES NOT ALLOWED	PREFERENCE
Add name and email to a list of valid emails to be sold to third parties.	PI_CO_TP
Add name and email of people who have more than one credit card to a list to be sold for advertising a real estate project.	PCP_CO_TP
Add email and age to a list of people to be sold to a company that sells food supplements.	PCP_CO_TP
Add email, height, and weight to a list of men and women who weigh more than certain amounts to be offered to plus-size stores.	PCP_CO_TP
If the registration is made from a mobile device, provide cell phone number and location to a company that specializes in offering advertising services based on location.	LO_CO_TP
Add name and email of the participant and date of the event to a list to be sold to restaurants near the location of the race.	LO_CO_TP

2) Case 1: Privacy Unconcerned Profile: In this case, the profile chosen by the user is Privacy Unconcerned and therefore all permissions are enabled. Thus, the service provider can perform all the secondary uses listed previously. The difference with Case 0, however, is that users, when requested to select a profile, are made aware of possible secondary uses and, when choosing the profile, consent the use of their data, which guarantees that there will be no violation of their privacy.

3) Case 2: Privacy Fundamentalist Profile: In this case, the profile selected by the user is Privacy Fundamentalist and therefore none of the afore mentioned secondary uses is allowed. Still, the service delivery would be possible, since there is no objection to using the data for its primary purposes (registering in the race, in this example). However, if the economic benefit of the SP is based only on the secondary use of data, it may not be interesting to provide the service under these conditions. Thus, to enable the service, the SP could request specific permission to use the data or charge a fee from the user or the event organizer, for example.

4) Case 3: Privacy Aware Profile: In this case, the profile chosen by the user is Privacy Aware and the secondary uses allowed and not allowed are presented in Table II.

5) Case 4: Privacy Pragmatist Profile: With the Privacy Pragmatist profile, the secondary uses allowed and not allowed are presented in Table III.

The two last cases, which concern the application of the Privacy Aware and the Privacy Pragmatist profiles, give rise to different behaviors of the SP, since the Privacy Aware restricts the secondary use of data by third parties, even if some offers of services are missed; and the Privacy Pragmatist, on the other hand, allows for greater use of data by third parties in order to provide access to a greater amount of personalized opportunities and services.

VI. PROTOTYPE

In order to verify the technical feasibility and the correct operation of the proposed mechanism and serve as the base for a future extension of an implementation of the OpenId Connect protocol, a prototype was developed. It is a Web application implemented in Java that allows to visualize through graphical interfaces the process of generation and encryption of the privacy token, as well as the communication between the IdP and the SP.

The prototype executes the processes that must be performed by the IdP to register users, collect their privacy preferences and store them; and, when requested by the SP, generate, protect with HMAC, encrypt and validate the privacy token.

The application also represents an SP that offers an online event registration service and its data collection and use applications, in order to show the effects of different user privacy preferences on the behavior of the service provider regarding the secondary use of their PII. This functionality has been included to implement the case study presented previously.

A. Implementation of the Prototype

The application comprises classes representing the IdP, the SP, the user, the user's privacy preferences, and the privacy token. The *User* object is defined by the user's personal data collected through a registration form in the IdP and the attributes of the *PrivacyPreferences* object are set with the values corresponding to the privacy profile selected or customized by the user. The values of the *PrivacyToken* object are defined by IDs of the IdP, the SP, and the user, by the user's privacy preferences, and by a timestamp of the moment the token was generated.

The IdP class has methods to generate, protect with HMAC, encrypt, serialize, and send a *PrivacyToken* object, which are called when the user uses his or her IdP registration to authenticate in a service provider. The SP class, in turn, has methods to receive the privacy token, request its validation to the IdP, decrypt it, and use it to define which secondary uses of data are allowed.

When the user wants to use the service, the SP requests the login to the IdP, which authenticates the user and creates a *PrivacyToken* object. This object is encoded into a JSON object, according to the code snippet shown in Figure 4, with the help of the Google GSON library, which makes it possible to convert Java objects to their JSON representations, as well as convert a JSON string into an equivalent Java object [21].

To be transmitted safely and efficiently, the JSON representation of the privacy token is used as the payload to create a JSON Web Signature (JWS) with the Nimbus JOSE+JWT library, which allows the creation and verification of JWTs [22]. This JWS is protected with HMAC using the SHA-256 algorithm and a secret key. The code snippet that generates the HMAC is shown in Figure 5.

After generating the HMAC, the JWS is used as the payload to create a JSON Web Encryption (JWE), which is encrypted with the Advanced Encryption Standard (AES) in the Cipher Block Chaining (CBC) mode of operation, with Public-Key Cryptography Standards (PKCS) #7, and an Initialization Vector (IV) of 128 bits. The code responsible for this encryption process is presented in Figure 6.

Finally, the JWE is subjected to a compact serialization that transforms it into a Base64 string, so that it can be transmitted easily and efficiently to the SP through URLs, for example. The complete generation and preparation process for transmitting the privacy token can be seen in Figure 7, which shows the successive states of the token and its transitions, as well as the technologies used.

B. Graphical Interface and Usage of the Prototype

The initial screen of the prototypeis divided into two parts: one corresponding to IdP, with options that allow registering, listing and editing users; and the other corresponding to the SP, with options to log in and register in a race. The user login option starts the sequence of generation, transmission and validation of the privacy token, which is shown step-by-step by the prototype. The option of registering in a race, in turn, is enabled only when the user is already authenticated and generates a report on the data collection and secondary uses according to the profile stored in the user's privacy token.

The registration page in the IdP asks for basic data of the users and allow them to select a predefined privacy profile or create a custom one. In order to verify the utility of the model in making users aware of the secondary use of their data and to allow them to define their preferences in a simple way, the sections of profile selection and profile customization were developed with a focus on good design practices and usability, and based on the recommendations in ISO/IEC 29100 [13].

This way, each profile is represented by a number, a name, an icon and a brief but expressive description. Also, colors are used to help differentiate the profiles and represent the levels of risks to privacy in each of them, being red for the profile with the highest risks and green for the one with the lowest risks. To provide users with more information about the possible uses of their PII and the chosen profile, the *View details* button shows the complete profile, i.e., all the privacy preferences with the corresponding settings. Figure 8 shows the section of the registration screen for selecting a privacy profile.

The Custom profile option leads to the page shown in Figure 9, which displays a checkbox for each privacy preference and allows users to check the uses of their data that they want to authorize. To guide and simplify the choice, users can also select one of the four predefined profiles as a basis for personalization. This same screen is shown in the option *View details* of the predefined profiles, but with the preferences already checked and disabled for editing.

On the SP's side, the Login option initiates the user authentication process and shows, through the graphical interface, all the steps that are triggered and the results that are generated, such as the structure of the JSON object, and of the token protected with HMAC.

The second option on the service provider's side opens a page for the authenticated user to register in a race, in which some additional data is requested and context information is also collected. Once the registration has been completed, the data obtained from the IdP, the data requested to the user, and the data collected from context are shown. Following is an analysis of possible secondary uses and the result is presented as a report that lists the secondary uses of data allowed and not allowed for the profile of the logged in user.

```
01    // Create GSON builder
02    Gson gson = new GsonBuilder().setPrettyPrinting().create();
03
04    // Create a PrivacyToken object
05    PrivacyToken privToken = new PrivacyToken(sp.getId(),
06                                              idp.getId(),
07                                              user.getId(),
08                                              user.getPrivPreferences(),
09                                              iat);
10
11    // Transform the PrivacyToken object into a JSON object
12    String tokenJsonString = gson.toJson(privToken);
```

Figure 4. Code snippet from the IdP class responsible for transforming the *PrivacyToken* object into a JSON object.

```
01    // Create payload with privacy token JSON string
02    Payload payload = new Payload(tokenJsonStr);
03
04    // Create HMAC signer
05    JWSSigner signer = new MACSigner(key.getEncoded());
06
07    // Create an HMAC-protected JWS object with a JSON object as payload
08    JWSObject jwsObject = new JWSObject(new JWSHeader(JWSAlgorithm.HS256),
09                                        payload);
10
11    // Apply the HMAC
12    jwsObject.sign(signer);
```

Figure 5. Code snippet from the IdP class responsible for protecting the provacy token with HMAC.

```
01    // Create a JWE object with signed JWT as payload
02    JWEObject jweObject = new JWEObject(
03        new JWEHeader.Builder(JWEAlgorithm.DIR,
04                EncryptionMethod.A128CBC_HS256)
05            .contentType("JWT")
06            .build(),
07        new Payload(jwsObject));
08
09    // Perform encryption
10    jweObject.encrypt(new DirectEncrypter(key.getEncoded()));
```

Figure 6. Code snippet from the IdP class responsible for encrypting the privacy token.

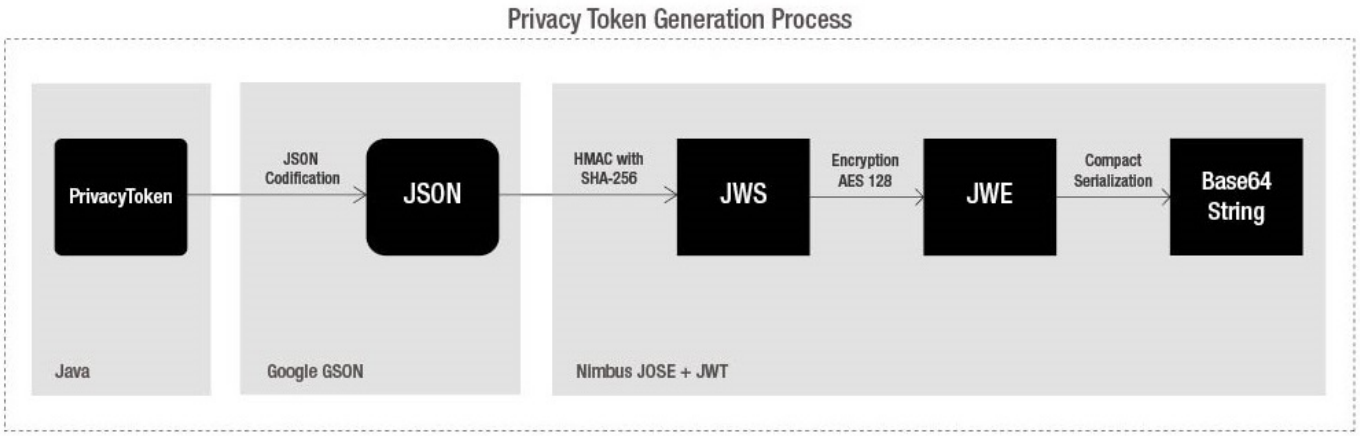

Figure 7. Generation process of the privacy token.

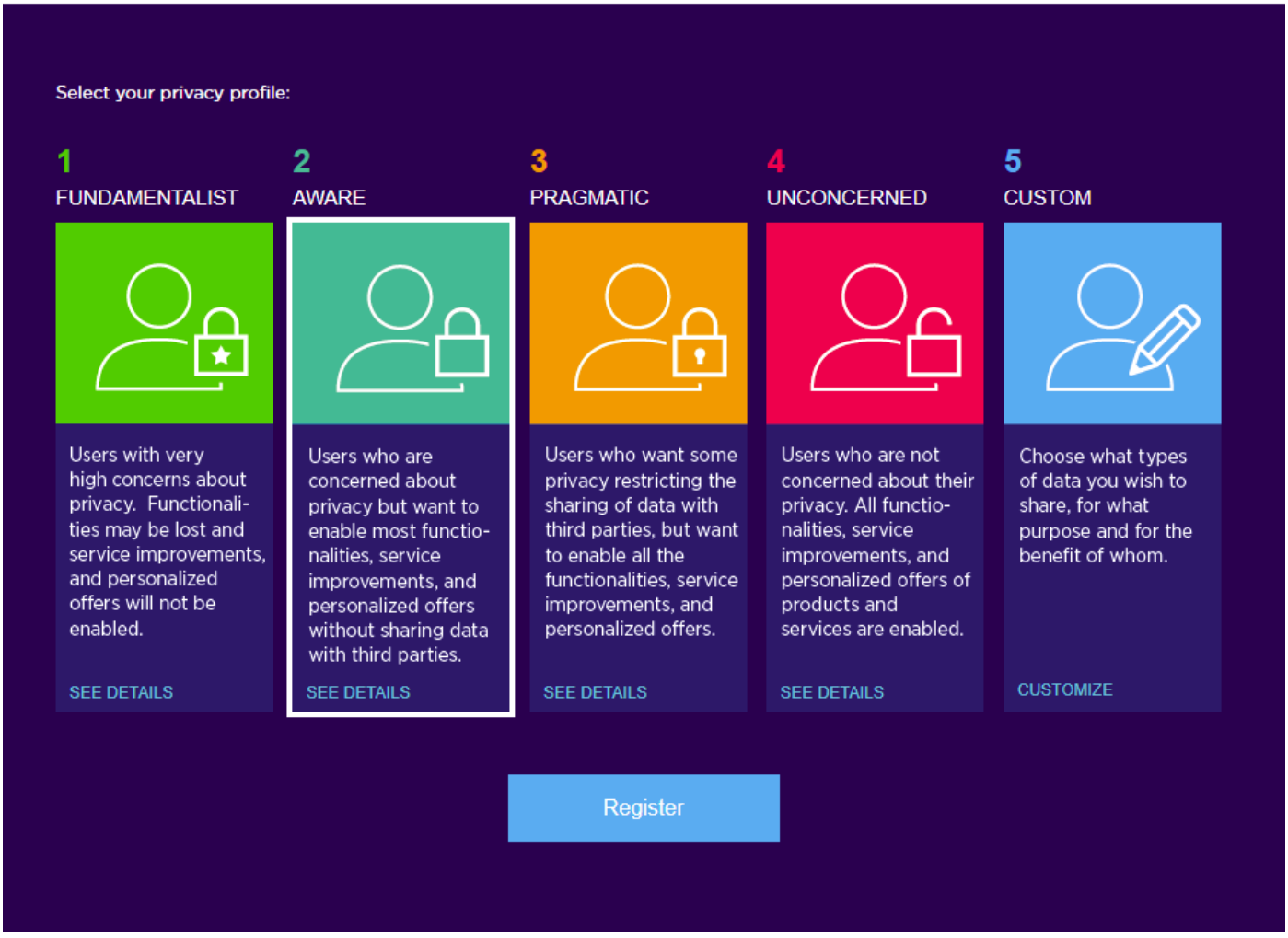

Figure 8. Prototype screen with the four predefined privacy profiles and the customizable one.

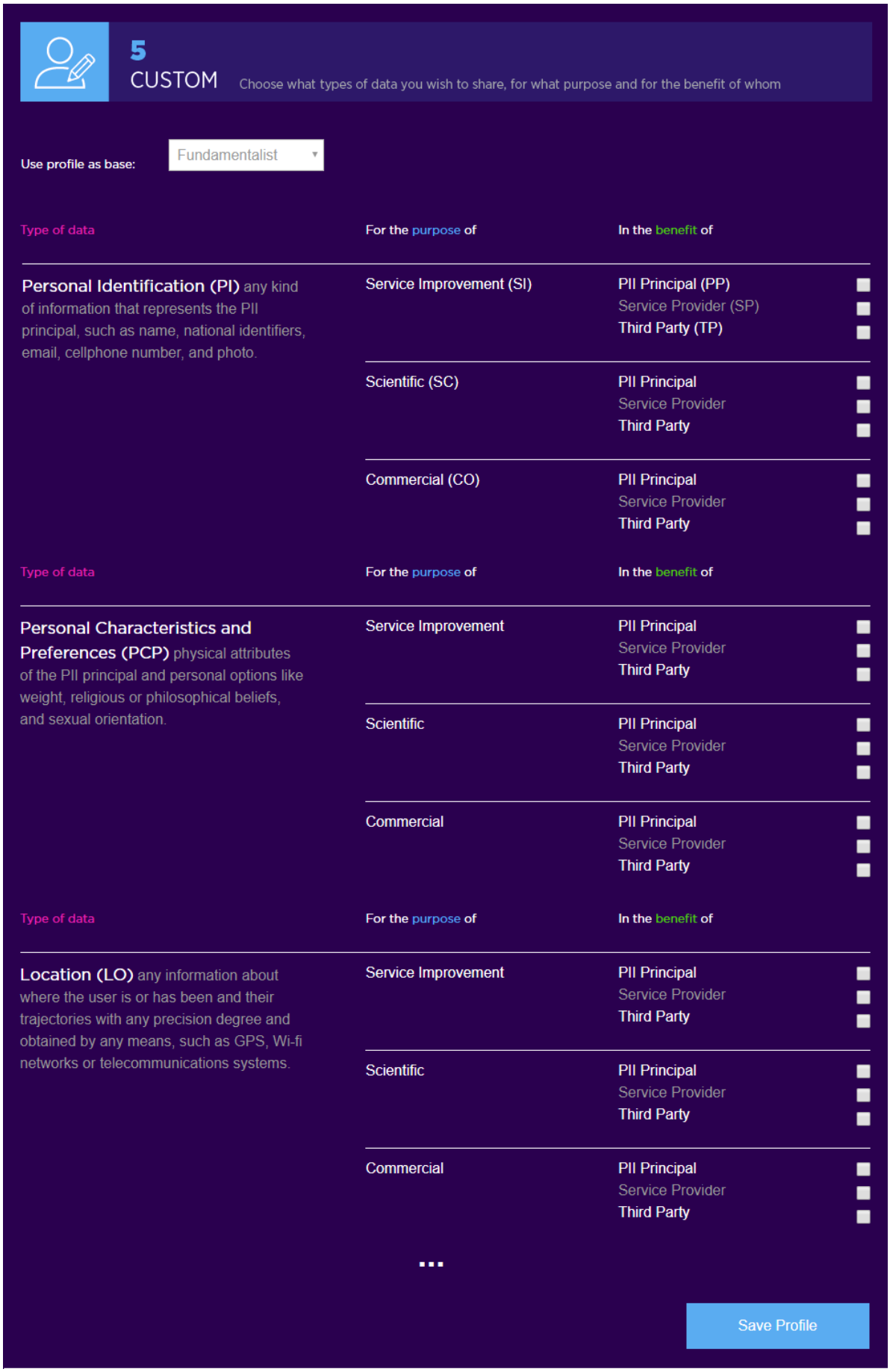

Figure 9. Part of the prototype screen that allows users to customize their privacy preferences.

VII. Conclusion and Future Work

In this paper, a practical mechanism that allows users to control how their PII can be used in a federated cloud environment was presented. The mechanism instructs them about the possible uses of PII by SPs, allows them to choose between four predefined privacy profiles or customize one, and sends their privacy preferences to the service provider.

This mechanism is based on a model that generically and comprehensively classifies the possible secondary uses of PII in three dimensions, which gives rise to a set of forty-five preferences that allow to control such uses. These preferences, which can be defined individually or through four predefined profiles, are encoded in a standardized, machine-readable format structure called privacy token, and sent to the SP along with the user's authentication data.

To the best of the authors knowledge, existing work focuses either on low-level approaches, such as privacy policy languages, which can be executed by machines; or on conceptual, high-level specifications, such as UML profiles, which provide a better understanding about privacy requirements in the development of systems and applications; or on complete architectures and models that aim to use the previous approaches to provide users with privacy. In addition, Shibboleth and OpenID Connect have privacy mechanisms that restrict the data that the user allows the IdP to send to the SP.

The aforementioned proposals, however, do not offer practical methods for users to define their preferences and send them to the SP and, in most cases, require the service provider to adopt specific technologies to represent their privacy policies. In addition, most are not suitable for federated cloud environments and do not provide resources for users to control the secondary use of their data, forcing them to accept the privacy policies established by the SPs.

The mechanism proposed in this paper, in turn, is user-centered, as it instructs users about the secondary uses of their data and helps them to control such uses. In addition, it can be easily adopted by users, IdPs, and SPs, as it does not require specific tools and knowledge from the users and is deployed with the technologies that the IdPs and SPs already use. Thus, an important feature is that it does not require service providers to use any specific standards to express and implement their privacy policies. It is only expected for SPs to adapt their data collection systems to interpret and fulfill the preferences expressed in the privacy token, which they can already read and understand once it has the same format as the other tokens used by OpenID Connect.

The applicability and the utility of the proposal were demonstrated by applying the model in a case study, and the technical viability and the correct operation of the mechanism were verified through a prototype that deploys the technologies for generation and transmission of the privacy token and implements the case study. The prototype also serves as the base for a future extension of an OpenID Connect implementation.

The proposed mechanism has the sole purpose of enabling users to control the secondary use of their PII allowing them to define their privacy preferences and sending them to the SP. Thus, it does not determine how the service provider will meet these preferences and enforce its privacy policies. For this, there are several approaches that can be used and there is no need for the SP to change those already adopted.

In addition, the mechanism does not define what data the identity provider can send to the service provider and how. Other mechanisms should be responsible for defining this, as the one proposed in [9] and the one already existing in OpenID Connect [20].

Although the use of the privacy token may create a need for negotiation between the user and the service provider, the proposed mechanism does not include methods for such a negotiation, since the latter is specific for a particular service and must be performed between the SP and the user without the need to modify the privacy token or involve the IdP.

The main contributions of this work are the preference specification model and the privacy token, which invert the current scenario where users are forced to accept the policies defined by SPs by allowing them to express their privacy preferences. These preferences are stuck together to their data and are used by the SP to align its actions or request specific permissions.

The proposal of this paper has been defined in order to extend the model presented in [9] and therefore can be incorporated into it as its mechanism for defining privacy preferences regarding the use and sharing of user's personal data. However, because of its simplicity and comprehensiveness and for using open technologies and standards, the model and the privacy token are not restricted to federated identity management systems and can be applied into any environment where it is needed to set user's privacy preferences.

As future work, we intend to extend an OpenID Connect implementation to support the proposed mechanism, as well as to analyze the impact of the token size on URL transmission and, if necessary, implement compression mechanisms. It is also proposed to perform usability tests to verify the effects of the model on users and to evaluate possible improvements in the classification of secondary uses of PII. Furthermore, it is proposed to assess the consequences for services, SPs and users of applying this mechanism in real federated cloud scenarios.

References

[1] M. E. Villarreal, S. R. Villarreal, C. M. Westphall, and J. Werner, "Privacy Token: A Mechanism for User's Privacy Specification in Identity Management Systems for the Cloud," in Proceedings of The Sixteenth International Conference on Networks - ICN 2017, Venice. IARIA XPS Press, Apr. 2017, pp. 53–58, ISBN: 978-1-612085-463.

[2] J. Zhao, R. Binns, M. Van Kleek, and N. Shadbolt, "Privacy Languages: Are We There Yet to Enable User Controls?" in Proceedings of the 25th International Conference Companion on World Wide Web, Montreal, Quebec, Canada. International World Wide Web Conferences Steering Committee, Apr. 2016, pp. 799–806, ISBN: 978-1-4503-4144-8.

[3] J. Iyilade and J. Vassileva, "P2U: A Privacy Policy Specification Language for Secondary Data Sharing and Usage," in Proceedings of the 2014 IEEE Security and Privacy Workshops, San Jose, CA, USA. IEEE Computer Society, May 2014, pp. 18–22, ISBN: 978-1-4799-5103-1.

[4] J. P. Kolter, User-Centric Privacy: A Usable and Provider-Independent Privacy Infrastructure. BoD Books on Demand, 2010.

[5] D. J. Solove, "A Taxonomy of Privacy," University of Pennsylvania Law Review, vol. 154, 2006, pp. 477–564.

[6] M. Benantar, Access Control Systems: Security, Identity Management and Trust Models. Springer, New York, 2006, ISBN: 978-0-387-27716-5.

[7] "OpenId Connect," 2015, URL: http://www.openid.net/connect/ [accessed: 2017-06-11].

[8] Shibboleth, "ConsentConfiguration," 2017, URL: https://wiki.shibboleth.net/confluence/display/IDP30/ConsentConfiguration [accessed: 2017-06-11].

[9] J. Werner and C. M. Westphall, "A Model for Identity Management with Privacy in the Cloud," in Proceedings of the 2016 IEEE Symposium on Computers and Communication (ISCC), Messina, Italy. IEEE, Jun. 2016, pp. 463–468, ISBN: 978-1-5090-0679-3.

[10] G. Alpár, J. Hoepman, and J. Siljee, "The Identity Crisis. Security, Privacy and Usability Issues in Identity Management," Computing Research Repository, vol. abs/1101.0427, 2011.

[11] D. Temoshok and C. Abruzzi, "Draft NISTIR 8149: Developing Trust Frameworks to Support Identity Federations," 2016, NIST, Gaithersburg, MD, United States.

[12] E. Bertino and K. Takahashi, Identity Management: Concepts, Technologies, and Systems. Artech House, Norwood, 2011, ISBN: 978-1-60807-039-89.

[13] "ISO/IEC 29100. International Standard - Information Technology - Security Techniques - Privacy Framework," 2011, URL: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123 [accessed: 2017-06-11].

[14] A. Westin, Privacy and Freedom. The Bodley Head, 1967.

[15] "OASIS Privacy Management Reference Model and Methodology (PMRM) Version 1.0," 2016, URL: http://http://docs.oasis-open.org/pmrm/PMRM/v1.0/PMRM-v1.0.html [accessed: 2017-06-11].

[16] F. Chanchary and S. Chiasson, "User Perceptions of Sharing, Advertising, and Tracking," in 11th Symposium On Usable Privacy and Security (SOUPS), Ottawa. USENIX Association, Jul. 2015, pp. 53–67, ISBN: 978-1-931971-249.

[17] "The Platform for Privacy Preferences 1.1 (P3P1.1) Specification," 2006, URL: https://www.w3.org/TR/P3P11/ [accessed: 2017-06-11].

[18] "Enterprise Privacy Authorization Language (EPAL 1.2)," 2003, URL: https://www.w3.org/Submission/2003/SUBM-EPAL-20031110/ [accessed: 2017-06-11].

[19] T. Basso, L. Montecchi, R. Moraes, M. Jino, and A. Bondavalli, "Towards a UML Profile for Privacy-Aware Applications," in Proceedings of 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), Liverpool, United Kingdom. IEEE, Oct. 2015, pp. 371–378, ISBN: 978-1-509001-552.

[20] OpenId, "OpenID Connect Core 1.0 incorporating errata set 1," 2014, URL: http://openid.net/specs/openid-connect-core-1_0.html [accessed: 2017-06-11].

[21] Google, "Google GSON," 2017, URL: http://github.com/google/gson [accessed: 2017-06-11].

[22] "Nimbus JOSE + JWT," 2017, URL: http://www.connect2id.com/products/nimbus-jose-jwt/ [accessed: 2017-06-11].