Enabling user privacy in identity management systems

Kheira Bekara, Maryline Laurent

Enabling User Privacy in Identity Management Systems

Kheira Bekara* and Maryline Laurent*

* CNRS Samovar UMR 5157, TELECOM SudParis, 9 rue Charles Fourier, 91011 Evry, France
{Kheira.Bekara, Maryline.Laurent}@it-sudparis.eu

Abstract *– The issue of user privacy is constantly brought to the spotlight since an ever increasing number of online services collect and process personal information from users, in the context of personalized service provisioning. This issue is emphasized in the identity management systems where user identities and profiles are valuable assets.*
Existing privacy legislative laws have to be brought down to the electronic world reality to limit the disclosure of personal data and avoid their misuse. This paper defines a privacy module for user's devices to automatically enforce privacy protection in identity management environments.

Keywords: *Privacy, Privacy policies, User control, P3P, XACML.*

I. INTRODUCTION

The growth of the Internet and the digitalization of the communication media allowed people and organisation to easily store process, analyse, and exchange personal data.

Personal identity (ID) and profile information are precious and valuable to organisations. On one hand, this enables personalising services with cheaper, faster and more effective interactions and transactions. On the other hand, misuses and unauthorised leakages of this information can violate user's privacy, cause frauds and encourage spamming.

As expressed in many surveys [1] [2], people are increasingly concerned about their privacy in the online electronic world. This concern is a natural consequence of the increasing number of individuals' privacy violation [3] [4], ubiquity and sharing information in IT systems, and the awareness of these problems.

Privacy is an important concern for all web services that require the user's Personal Identifiable Information (PII). It is even more critical in the digital Identity Management Systems (IMS), which are based on naturally exchanging attributes of users between Service Providers (SP) and Identity Providers (IDP). One should have in mind that the success of such systems is directly linked to the trust of the users in the system to manage their personal data preserving privacy.

In this paper, we define Identity Management Systems (IMS) as "the business process that creates, manages, and uses the IDs, and the infrastructure that supports that process."- Burton Group [5]. Also we refer to the federated IMS [6] vocabulary to define the Service Providers (SPs) which offer some services to the registered individuals or users, Identity Providers (IDPs) which role is to manage the individuals' identities, Circles of Trust (CoT) which enable users after a single authentication to access to services of different SPs belonging to the CoT, and Attribute Providers (APs) which role is to store user's related attributes in a predefined CoT. Finally, we restrict the definition of the identity given in [7] to the digital representation of the set of one or more attributes known about a person.

This paper proposes a (middleware-level) privacy module to assist users and give them tools to ensure control on their personal data. The proposed privacy module is expected to run at the user's device, and helps users to automatically fulfil legislative requirements.

In this paper, we assume that the user and the SP have already defined their own privacy policies before a transaction is taken place. That is, the SP specified the personal attributes that the user is required to deliver to SP under some specific P3P policy conditions [8]: the retention period during which the attributes are stored by SP, the use purpose which expresses one or more intentions for the collection or use of data, and the recipients which the attributes might be delivered to. Moreover, the user defined his/her privacy preferences, i.e. for each service type (e.g. e-commerce services), the personal attributes (e.g. address, CC_Number) that he/she is authorizing to deliver under specific P3P conditions (retention, purpose and recipient).

This paper is organized as follows. Section II introduces privacy legal aspects for personal data protection. Section III briefly presents the privacy risks related to IMS. Sections IV and V describe our privacy architecture model including its functions and components. Section VI illustrates the operations done by our privacy module with an e-commerce use case. Section VII gives conclusions, and acronyms are listed at the end of the paper.

II. LEGAL ASPECTS

The first data protection act, adopted in 1970 by the West Germany state, set in motion a trend towards adopting privacy legislation. The US Privacy Act [9], adopted by the Congress in 1974, was the first influential text. Nowadays, the European Directive 95/46/EC [10] enforces a standard for strong data protection and it is the most influential piece of privacy legislation worldwide, affecting many countries outside Europe in enacting similar laws.

The most fundamental requirements related to personal data protection, with respect to lawfulness and fairness, based upon the EU legislation [10] and the OECD guidelines [11], can be summarized as follows:

- Personal data must be collected only for specified, explicit, and legitimate purposes.
- Processing of personal data should take place if necessary only.
- The personal data subject has given his consent unambiguously.
- All the appropriate security safeguards must be provided to ensure adequate treatment of user data.
- Personal data should not be further retained or disclosed to third parties, except with the knowledge and the explicit consent of the data subject.

The recent European legislations [10], [12] require that users must be informed and aware of the privacy policies that will apply on their personal data for collection, usage, and dissemination in case they reveal them.

The aforementioned privacy principles and requirements can't be sufficiently protected neither by privacy related legislation, nor by data collectors' self-regulation. Privacy enforcement should take place by technical means. These means should target the minimization of the amount of personaly identifiable data that are collected, as well as the enforcement of the privacy agreement between data collectors and personal data subjects.

III. PRIVACY RISKS IN IMS

The risk analysis is based on the ID life cycle [13], illustrated in Fig. 1 and including the propagation, use, maintenance and removal processes.

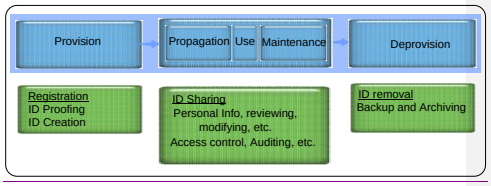


Fig. 1. ID Life Cycle

A. ID provision risks

ID provision process includes two main processes: the user ID registration, and ID right assignment.

The first process includes an ID proofing process. In this process, the IDP requires PII from the user for ID proofing. If the IDP collects more PIIs than needed or carelessly manages the collected PIIs, this can raise some privacy concerns. To counteract this threat, the user should be notified about the use purpose of the PIIs requested during ID proofing, the PII retention period, and the technical and administrative measures for protecting collected PIIs.

The second process includes the ID creation and right assignment. During this process, the ID and the related credentials (authentication information) are created and user privileges are assigned to the ID. Also, the IDP creates new PIIs linked to the user during this process by creating ID to identify the user, as well as other ID related attributes. Therefore, the association that can be done between the afomentionned elements is highly critical from a privacy point of view. In case some of the PIIs are disclosed, there is interest for IDPs in issuing anonymous ID to the user like with anonymous certificates.

B. ID propagation, use, and maintenance risks

In order f~~rom~~or the services of SP's of other CoT's, the user should use and propagate the ~~created~~ issued ID from the original CoT to the visited CoT. This latter uses the ID to support the authentication/authorization operations before granting users access to SPs. As such, ID and ID related attributes are stored and maintained in the visited CoT during the retention period.

Three main functions are provided by the IDP during this process: storage of ID and related attributes, ID propagation, and ID access and modification.

During the storage process, some PIIs can be disclosed by the AP or SP affiliated to the CoT of the IDP, if the access rights to PII are incorrectly configured. Therefore, the access rights should be tightly controlled.

During the ID propagation process, the user ID is distributed among several CoTs, so that the ID and ID related attributes can be used by them, and illegal leakage of them might happen. That is why, it is recommended to analyse the security and privacy guarantees offered by the visited CoTs and SPs, and whether they expect to share the ID-related attributes and PIIs with other entities.

The process to access to the IDP, offers the users the possibility to get and modify their IDs, ID related attributes, and PII stored and managed by IDPs. Hence, the IDP should provide the method for retrieving and modifying the user ID, related attributes, and PII through a proper and secure procedure. However, only the owner of the information, and the authorized administrators should be assigned the retrieval and modification privileges on the ID and PII. Note that wrong assignment of the privileges can lead to PII disclosure.

C. ID removal risks

The removal process consists in removing the invalid ID registered in the IDP, as well as the ID related user account, the attributes, PII, privileges given to ID and related logs. If any privilege is left for the deleted ID in the CoT, it can cause serious security vulnerabilities in that CoT. If ID, attributes, or PII on the remote user are not deleted, or the information related to the valid user is deleted intentionally or mistakenly, they all can be a privacy threat. Therefore, some verification procedures or technical measures are required to control whether an ID removal operation is legitimate.

IV. PRIVACY RELATED FUNCTIONS

Policy definition function
This function helps the users defining/modifying their privacy preferences through drop down lists. The resulting policy is stored under a policy file specified into a specific XPACML language (eXtensible Privacy Access Control Markup Language) we defined. The XPACML language is based on XACML [14] and is published in [15]. It helps defining the privacy preferences of the users for each of their data attributes and for each service type.

Decision function
This function generates an automatic authorization (or denial) access decision, by checking the compatibility between the SP privacy policy, the legislative policy, and the privacy preferences defined by the user for a specific data element and a service type.

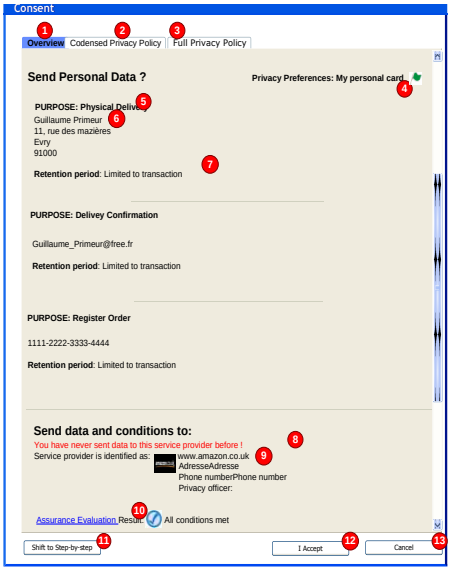
Negotiation function
This function generates counterproposals in case conflicts occur between the user preferences and the SP policy. The counterproposals are automatically built based either on data type substitution, or on privacy policy terms. That is, the module is proposing to SP either a less precise data attribute with less restricted policy, or the required attribute with a restricted P3P policy compliant to the user preferences. Note that this function is an advanced feature of the privacy module as it requires the SP to be equipped with a privacy module as well so the SP is able to handle the counterproposals.

Notification function
This function is to notify the users about the policy that applies to their personal data requested during the transaction.

Consent function
This function requests the user's explicit consent through the two following windows (see Fig. 2):

- The simplified consent window.
- The advanced consent window which contains the privacy policies instructions with three levels of details (overview, medium, condensed). This decomposition of the SP's privacy policy into three levels enables the advanced users to get the detailed policy and the novice users to get a simplified version of it.

Log function
This function stores the history of the transactions. Each transaction is uniquely identified with an identifier « Id » bound to the policy set that applies to it.



1. Overview tag: summary of the requested attributes, the purposes and retention period for which they are requested by the SP

2. Condensed privacy policy tag: a second level presentation of the privacy policy of the SP
3. Full privacy policy tag: the complete privacy policy of the SP
4. My personal card: the name of the card in use for the transaction. Clicking on the flag gives access to the profile: "My personal card"
5. Purpose: goal for which data are requested
6. Value: the value of the requested attributes, given by the selected card
7. Retention period: period during which the data will be stored by SP
8. Alarm: warning messages to the user
9. Information: SP related information
10. Assurance level: minimal assurance level given by the SP
11. Shift to Step-by-step: advanced users have the possibility to get the SP's privacy policy and validate that policy step by step
12. I Accept: acceptation of the SP's privacy policy
13. Cancel: cancel the current transaction

Fig. 2. User Consent Window and Associated Legend

V. COMPONENTS OF THE PRIVACY MODULE

The policy based privacy middleware is hosted at the user's device. Fig. 3 gives the full internal architecture with its privacy components. Our framework is usable for any IMS model, but Fig. 3 and 4 give illustrations on the user-centric model, that is, the model investigated by Microsotf (ex: Microsoft CardSpace) which introduces an identity selector and an InfoCard wallet at the user's side.

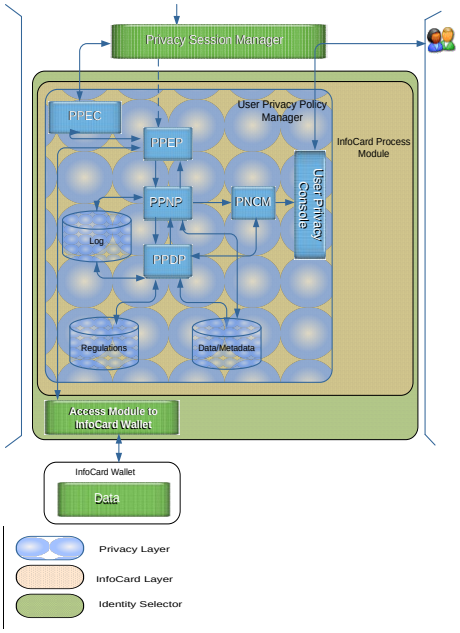
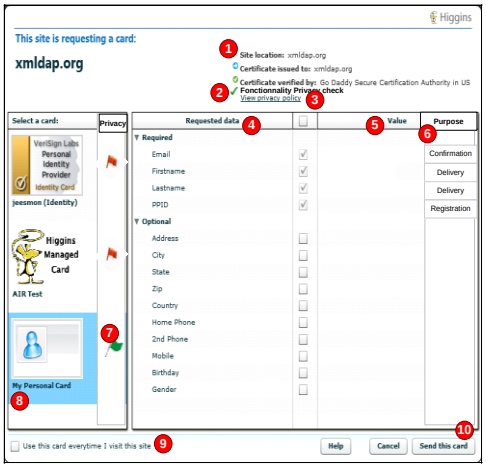


Fig. 3. Privacy Architecture in the User-Centric Architectural Model

The Privacy Session Manager

It represents the privacy user interface. This component can be integrated into the identity selector. The Privacy Session Manager component interacts with the SP to get its privacy policy. As soon as the SP's privacy policy is obtained, the policy is forwarded to the PPDP for comparison with the legislative policy and then with the user's privacy preferences. When the result of the comparison is get back, the Privacy Session Manager with the help of the PNCM component, displays to the user the privacy status of the SP (see Fig. 4). It also displays the required attributes by the SP, the purpose for which they are collected, and a privacy check flag of the compatibility of the user preferences related to his/her cards against the SP's policy. Thus the user can control his/her attributes that are to be communicated to the SP, and can decide to transmit the mandatory attributes only.

Before accepting the transaction, the user can view the SP's privacy policy through the windows of Fig. 2 by clicking on the privacy policy link (#3 of Fig. 4). He can also display the SP's privacy policy related to the required attributes by clicking on one of the flags next to the card (cf. Fig. 4). Only the cards with compatible preferences are activated for the selection.



1. Site location: the information about the SP requiring the user's attributes
2. Privacy status: the status computed after localy checking the SP's privacy policy against the user's preferences
3. Privacy policy: link to the SP's privacy policy
4. Requested data: mandatory and optional requested attributes
5. Value: value of the requested attributes which ~~are~~ is not yet filled
6. Purpose: purpose for which attributes are requested
7. Privacy check flag: compatibility check of the SP's privacy policy against the profiles attached to the cards

8. Personal card: the personal card which preferences are compatible with the SP's privacy policy is preselected by the system. In Fig.4, only the third card "My Personal Card" is compatible, as shown by the privacy check flag
9. Use everytime: possibility is given to the user to fix a specific card (hence, a profile) for the next transactions with the same SP
10. Send this card: global consent by the user to send the required attributes bound to the card

Fig. 4. Identity Selector Showing the Attributes Requested By the SP and Associated Legend

User Privacy Policy Manager (UPPM)

UPPM is the specific software that handles the user's interaction with the IMS components. This includes interactions like adjusting the privacy level, informing the user about the activated privacy protections, editing privacy preferences for each user's card/profile, and providing feedback messages.

The necessity of the UPPM first of all comes from the diversity of the types of managed private information. In order to come up with a privacy-aware solution, the different aspects of private information need to be specified, categorized and structured. The UPPM's first responsibility is to structure private information into a data category to be communicated to the IMS components (ID selector). As such, the UPPM implements the following interfaces:

1. A friendly intuitive User Interface, called "User Privacy Manager Console" (UPMC), through which the privacy level, and privacy preferences are set. Privacy related alerts can also be provided to the User.

2. An interface with IMS components for the provision of private information and privacy policies and interaction between the User and the SP (grant/deny permissions, check privacy status, etc.).

Privacy Policy Enforcement Point (PPEP)

This component receives all the requests to access protected data and decomposes the ClaimsRequest coming from the SP requesting several attributes into several ClaimRequests, each one asking for one attribute. Next, it sends each single ClaimRequests to the PPNP, and then to the PPDP to obtain the authorization needed to deliver data. In fact, the PPEP forges a request for the authorization, specifying the sender of the request, the type of service, the type of data claimed and all other information needed by PPDP in order to elaborate a decision. After the decision is made, the PPEP gathers the single responses issued by the PPEP, to produce an overall decision.

Privacy Policy Decision Point (PPDP)

The PPDP is the entity that takes a decision about the personal data delivery to SP. It looks up the legislative policy that applies for that service type and the privacy preferences set by the user for decision making. Then it evaluates both policies and returns its decision to the PPEP. The authorization can be given, or rejected or an error can occur in the case that the PPDP doesn't find any policy for the particular service.

Privacy Policy Negotiation Point (PPNP)

The PPNP performs the negotiation of the SP privacy policy, and the user privacy preferences. Note that the PPNP full usage requires the SP to be equiped with a similar PPNP component for the negotiation process to take place.

After receiving a service request from the PPEP, the PPNP checks whether the request is permitted by forwarding the message to the PPDP. If it is permitted, the PPNP forwards the message to the PPEP. Otherwise, the PPNP starts a negotiation process with the SP until a termination signal comes from any parties. The objective of PPNP is to solve the occurred conflicts by implementing the negotiation function presented in section IV.

Finally, the PPNP sends a XPACML response message back to the PPEP and the PPEP enforces the decision by allowing or denying delivery of personal attributes.

Privacy Notification and Consent Manager (PNCM)

The PNCM undertakes all the tasks related to user's notification and consent. It is implementing the consent function described in section IV using few consent windows. This component is also designed to warn the user about possible privacy abuse so the user decides whether to continue the transaction.
For the negotiation process, this component is used to ask the user decision about a conflict after running the whole automated negotiation process.

Privacy Policy Envelope Constructor (PPEC)

The PPEC assembles the user's personal data with their privacy related metadata into an encrypted and signed privacy envelope that is transmitted to the SP.

Databases

Regulation database

The regulation database includes the regulation privacy policy for each personal data and the type of the service related to.

User preference database (metadata)

This database contains the user's privacy preferences related to the different data type and service type categories.

Log database

It is a database permitting backup of the history of the completed transactions. For each transaction with a particular SP type, two files are stored, one including the data elements with an autorization access, and another one including data elements with a non-

authorized access. These files are later useful for the negotiation process.

VI. E-COMMERCE USE CASE

This section illustrates the operations done by the proposed framework with an e-commerce use case ~~on~~ in an IMS user-centric ~~model~~ environment~~with an e-commerce use case~~. We assume the user is visiting the site of an SP for the very first time.

Fig. 5 illustrates the resulting policy based privacy architecture and service provisionning steps. The procedure starts with the user requesting the e-commerce service. Upon receiving the request, the SP asks for some personal data (PDRequests) in order to achieve the requested service. The SP asks for the needed personal data through a ClaimsRequest that contains an "Object" tag (to launch the identity selector) and a P3P header that helps locating the SP's privacy policy (e.g. URI) for the requested service.

~~selector) and a P3P header that helps locating the SP's privacy policy (e.g. URI) for the requested service.~~

Mis en forme : Retrait : Gauche : 0 cm

Fig. ~~3~~5. Sequence Diagram of Data Flows between the User and the SP

~~Therefore, the Identity Selector is displayed to the user with the compatible cards of the wallet and the mandatory required attributes (and the optional ones). As shown in Fig.4, several flags are displayed to give to the user an overview of the cards which can be used to interact with the SP (the preferences match with the~~

~~selector) and a P3P header that helps locating the SP's privacy policy (e.g. URI) for the requested service.~~

Upon receiving the request from the SP, the PPDP component of the policy based privacy architecture checks the validity of the SP's data request policy against the regulatory policies and the user privacy preferences. It ~~displays some of this privacy related~~

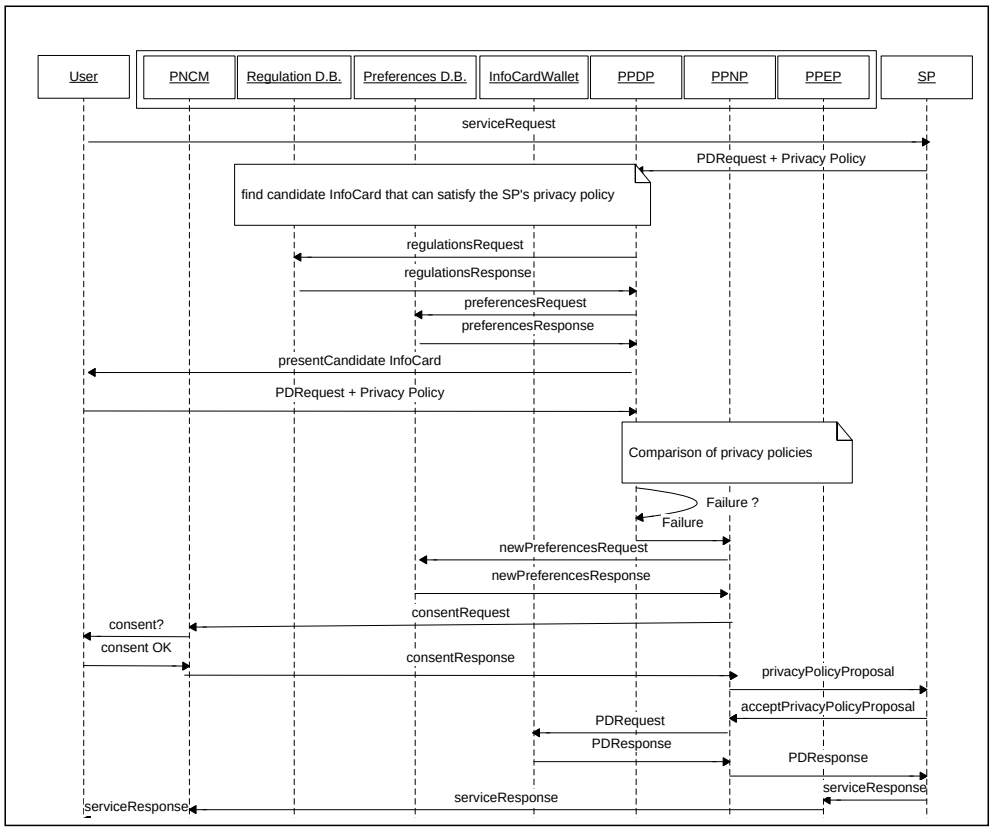


Fig. 5. Sequence Diagram of Data Flows between the User and the SP

~~information on the user's identity selector interface~~ helps the Identity Selector to preselect and display to the user the compatible cards of the wallet and the~~.~~ mandatory required attributes (and the optional ones). As shown in Fig.4, several flags are displayed to give to the user an overview of the cards which can be used to interact with the SP (the preferences match the SP's privacy policy).

~~Upon receiving the request from the SP, the PPDP component of the policy based privacy architecture checks the validity of the SP's data request policy against the regulatory policies and the user privacy preferences. It displays some of this privacy related information on the user's identity selector interface.~~

Mis en forme : Retrait : Gauche : 0 cm

~~SP's privacy policy).~~
If policies are compliant, the access is granted to the requested service, otherwise, the request is transmitted to the PPNP for resolving privacy policy conflicts. The new privacy policy proposal is then sent to the SP privacy policy manager. If the privacy policy proposal is accepted by SP, the access to the requested service is granted and a serviceResponse is sent to the user.

VII. CONCLUSIONS

This paper presents the privacy related issues in the IMS, and our policy based framework for ensuring the protection of the personal data in the IMS. The description of our privacy enabling middleware and our privacy enabling architecture for identity management environments is given. The main idea of this approach is the integration of all the privacy-critical functions into a privacy-proof middleware policy. It helps maintaining the privacy during all the three phases of any communications between entities: pre-communication, communication and postcommunication.

This framework refers to the current privacy legislation and proposes a technical solution to enforce that legislation.

A prototype of the proposed framework is under implementation, and is likely to be integrated into a full user centric IMS. Complementary research works are also investigated on a privacy policy language supporting privacy policy exchanges between SP and user, privacy access control on the user personal data and privacy policy negotiation.

ACKNOWLEDGEMENTS

This research is part of the project called FC2 (Federation of Circles of Trust - www.fc2consortium.org). Authors are thankful to DGCIS (Direction générale de la compétitivité de l'industrie et des services) for financially supporting TELECOM SudParis.

ACRONYMS

AP ___Attribute Provider
~~COT~~ COT __Circle Of Trust
IDP ___IDentity Provider
IMS ___Identity Management Systems
PII ____Personal Identifiable Information
SP ____Service Pprovider

REFERENCES

[1] J.B. Earp, and G. ~~J.B. et~~ Meyer, ~~G. (2000)~~ "Internet Consumer Behavior: Privacy and its Impact on Internet Policy", 28th Telecommunications Policy Research Conference, Sept. 23-25, 2000.
[2] A. Kobsa, ~~A. (2002).~~ "Personalized hypermedia and international privacy." Communications of the ACM, 45(5), pp. 64-67, 2002.
[3] Synovate (2003) Identity Theft Survey Report, prepared for the Federal Trade Commission (FTC), ~~.~~ Sept~~ember~~. 2003. ~~En ligne: http://www.ftc.gov/os/2003/09/synovatereport.pdf~~
[4] Javelin Strategy & Research (2005), 2005 Identity Fraud Survey Report, Jan~~uary~~ 2005, ~~En ligne : http://www.javelinstrategy.com/reports/2005IdentityFraudSurveyReport.html~~
[5] http://www.uits.iu.edu/page/aptr
[6] S.S.Y. Shim, G. ~~, S.S.Y., Geetanjali~~ Bhalla, V. ~~Vishnu~~ Pendyala ~~(2005)."~~ Federated identity management ~~"~~. Computer. Volume 38, Issue 12, pp ~~Dec. 2005:~~ 120-122, Dec. 2005 ~~pp~~
[7] ICPP/ULD Schleswig-Holstein and SNG, "Identity Management System (IMS): Identification and Comparison Study", 2003.
[8] L. Cranor, B. Dobbs, S. Egelman, G. Hogben, J. Humphrey, M. Langheinrich, M. Marchiori, M. Presler-Marshall, J. Reagle, M. Schunter, D. Stampley, and R. Wenning, "The Platform for Privacy Preferences 1.1 (P3P1.1) Specification," W3C Working Group Note, ___Nov~~ember~~. 2006. ~~[Online]. En ligne: http://www.w3.org/TR/P3P11/~~
[9] U.S. Public Law No. 93-579, Dec.31, 1974, 5 U.S.C. 552a.
[10] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L No.281, 23 Nov. 1995. ~~En ligne: http://www.cdt.org/privacy/eudirective/EU Directive .html~~
[11] Organization for Economic Co-operation and Development, "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", Sept.1980.
[12] Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, brussels. Official Journal L No.201, 31 Jul. 2002. ~~En ligne: http://www.etsi.org/public-interest/Documents/Directives/Standardization/Data Privacy Directive.pdf.~~
[13] ~~Dean~~ D. Tompson, "Identity Management : Concepts, technology and application of Identity Management for eHealth", Sun Microsystems.

Mis en forme : Anglais (Royaume-Uni)
Commentaire [ML1]: J'ai homogénéisé en fonction du format pour ICITIS
Mis en forme : Police :(Par défaut) Times New Roman, Anglais (Royaume-Uni)
Mis en forme : Police :(Par défaut) Times New Roman
Mis en forme : Police :(Par défaut) Times New Roman, Anglais (Royaume-Uni)
Mis en forme : Allemand (Allemagne)
Mis en forme : Anglais
Code de champ modifié
Mis en forme : Anglais
Mis en forme : Anglais (Royaume-Uni)
Mis en forme : Français (France)
Mis en forme : Anglais
Code de champ modifié
Mis en forme : Français (France)

[14] eXtensible Access Control Markup Language (XACML), Version 2.0, OASIS Standard, 1 Feb. 2005, http://docs.oasisopen.org/xacml/2.0/access_control-xacml-2.0-core-specos.pdf.
[15] K. Bekara, K., Y. Ben Mustapha, Y., and M. Laurent, M., (2010) "XPACML eXtensible Privacy Access Control Markup Language ", Second International Conference on Communications and Networking (ComNet'2010), Tozeur, Tunisia, Nov., 2010.