Privacy preserving in finer-grained access control using XACML and OpenID Connect

Gerson Luiz Camillo*,Carla Merkle Westphall

Departamento de Informática e Estatística (UFSC-CTC-INE),
Universidade Federal de Santa Catarina,
Laboratório de Redes e Gerência,
CEP 88040-900 - Campus Universitário Florianópolis, Santa Catarina, Brasil
Phone: +55 048 3721-
E-mail: gerson.camillo@posgrad.ufsc.br
E-mail: carlamw@inf.ufsc.br
*Corresponding author

Abstract: Many service providers have started implanting personalization in their web portal so that an individual needs not only to submit the assurance of digital identity but also to reveal Personally Identifiable Information (PII), known as attributes in the context of control access. The disclose of PII represents a privacy problem. This paper offers a model that allows for the individual to obtain services without the need to report PII, but only the results of the politics of fine granulation over the value of the attribute. We also present an implementation of a prototype in addition to a case representing a hypothetical scenery for evaluation. The project demonstrated that for certain situations an user can restrict the publication of certain PII and still gain access to services.

Brings the fine-grained authorization to the world of open and lightweight identity management through the use of XACML 3.0 and OpenID Connet.

Keywords: access control; XACML; federated identity management; OpenID Connect; privacy preserving.

Reference to this paper should be made as follows: Camillo, G.L. and Westphall, C.M.. (2015) 'Privacy preserving in finer-grained access control using XACML and OpenID Connect', *Int. J. Security and Networks*, Vol. x, No. x, pp.xxx–xxx.

Biographical notes: Gerson Luiz Camillo received his BSc in Computer Science from the Universidade Federal de Santa Maria, RS, Brasil. His research interests include security, access control and identity management.

Carla Merkle Westphall is a Professor in the Departamento de Informática e Estatística of Universidade Federal de Santa Catarina (UFSC) Brazil. She is working in security since 1996. Her research interests include information security, distributed security, identity management and cloud security. She received her PhD in Electrical Engineering (Information Systems Security) from the Universidade Federal de Santa Catarina. She is a member of the Networks and Management Laboratory which has many master and doctoral students developing security research.

1 Introduction

The technologies of authentication and authorization have been evolving in matters of security, usability, and performance in order to accommodate to the context of service distribution in the web. The browser became the main interface to the utilization and diffusion of information, as well as to the access to online resources. The data that identifies and distinguishes the user have acquired inestimable value in the digital society, to the extent that any transaction online usually requires that some information is disclosed. This data is represented by attributes and is known as Personally Identifiable Information (PII). The relationship between the traces we leave while navigating on the Internet and the information that identifies us has allowed the development and rising of Internet giants such as Google and Yahoo.

MOTIVAÇÃO: por que é importante PRIVACIDADE. The privacy aims to control and protect both data owns by a user and the PII proving law, techniques and mechanisms to empower the entity about its information. Specificaly, in the area of computer security, privacy is about minimizing the personal information released and/or prevent that attributes has been linked to the user (Gürses, Troncoso and Diaz, 2011; Heurix et al., 2015; Landwehr et al., 2012). Privacy was subject a concern a long time ago. The importance of protect personal data levou às primeiras iniciativas de regulação. And the first

normative was established in 1981 with guidelines to protect the privacy of personal data in EU (Organisation for Economic Co-operation and Development, 1981) with the establishment of eight principles. These principles influenced the criation of directives, laws and frameworks around the world. The importance of privacy today is reflected in the revision of the guidelines (Organization for Economic Co-Operation and Development, 2013) and the consequences in the form of companies work with personal data (Kuschewsky, 2014).

POR QUE É IMPORTANTE RESOLVER O PROBLEMA: exemplos de aplicações To understand the driving problem [driving problem of what?] we present the scenario of a library, as used in the paper of (Camenisch et al., 2014). The librarian cannot lend titles (books, films) to underage persons. To further the community use, the library will send free of charge books to people who are 60 or older and who live in the central area of the city. Considering the service will include the option of preserving the privacy of user data, how can we create a solution that allows the individuals to use the service without exposing personally identifiable data? This question comprises two sides of service negotiation: the service provider needs to guarantee the restriction on using some services and the user doesn't want to disclose personal information.

O QUE O PRESENTE TRABALHO TEM DE INOVADOR em relação aos outros trabalhos, CONTRIBUIÇÃO: The above problem prompted the search of related works and systems that presented solutions to achieve privacy in the use of online services. The context of the problem and the proposals of this work parallel service provider (SP) enforcing fine-grained policies [and] personally attributes managed by an identity provider (IdP). Both are executed in disjunct security domains. Specifically, the SP runs XACML and the IdP, OpenID Connect, under Representational State Transfer (REST) services and protocols. The only paper that handled with these devices in the setting of privacy preserving was (Ma and Sartipi, 2015), but in that case, the policy manager was in the same domain of the identity provider. The Privacy-preserving Attribute-based Credentials (Privacy-ABCs) technologies Camenisch et al. (2009); Dagdee and Vijaywargiya (2011) offers solutions for privacy-preserving of PII robustness of underlying cryptography, but is a complex system. The User-Managed Access (UMA) profile of OAuth 2.0 Hardjono et al. (2016) is an alternative to authorization in Web 2.0 that can be integrated with OpenID Connect bringing novel perspectives to user management of control access. But UMA depends strongly on the user defining policies and on the resource server to enforce such policies (there is a step that establishes a trust relationship between the entities).

We present in this paper a different approach, that permits the user to minimize the personal information released to the service provider resource server while still maintaining access to resources/services. It is not necessary to trust the service provider because it trusts the user possesses the required attribute. The idea has similarities with the Privacy-ABC technologies, but the proposed model is supported by recent protocols and specifications, like OAuth 2.0, OpenID Connect for identity management and RESTful as the means of transportation. Aside, the service provider applies fine-grained authorization using XACML architecture and policies.

The main contributions of this work are: introduction of a framework that evaluates attribute-based access control policies in the identity provider, returning to the service provider only the results of the evaluation, aiming to prevent the service provider from obtaining private user data; the enforcement by the service provider of fine-grained access control policies using XAML while keeping user privacy regarding PII; and the proposal of a prototype to assay a use case scenario.

The remaining of this paper is arranged as follows: Section 2 presents the related works; Section 3 discusses access control, identity and privacy; in Section 4 the proposal is presented; Section 5 exposes the development; the results are displayed in Sections 6 and 7 has some summing-ups and the description of future works.

2 Related works

There are a broad range of solutions to enhancing privacy in systems that delivery services using or providing data relative to a person. The systems are known Privacy Enhancing Technologies (PET). A lot of PET and proposals have the purpose of augment or stablish privacy in the relationship between users and service providers when some form of personal data is involved. The range start with Cookie-cutters blocking cookies and language privacy of Platform for Privacy Preferences (P3P) ending with cryptographic solutions using including third-party authorities, such as the Privacy-Attribute Based Credentials (Privacy-ABC). To restrict the works to analyse and compare, we restrict to the privacy of personal data, as defined in EU Directive 95/46/ECEU Directive (1995) that refers to the piece of information that identifies directly or indirectly a natural person. As we are working on data minimization, the scopes left out the proposes that treats how data is used, according to (Mondal et al., 2014).

(Kolter, Schillinger and Pernul, 2007) foi um dos primeiros trabalhos que buscou resolver a questão de privacidade em sistemas de controle de acesso baseados em atributos sobre Service-oriented Architectures (SOA). O autor estendeu a plataforma XACML para suportar PDPs separados do provedor de serviço. Essa arquitetura permite que o usuário, ao acessar o serviço, defina qual sua preferência de privacidade, o que determina a escolha do PDP mais adequado. Mas isso requer que o provedor de serviço confie na decisão gerada pelo respectivo PDP. Questões de confiança

no transporte de autorizações foram resolvidas através de infraestrutura de chaves públicas. Um importante conceito apresentado foi de associar diferentes PDPs a perfis de privacidade, however the paper don't present a prototype because the model was planed to included in project Access-eGovPernul (2009).

An approach to privacy preserving PII is the authentication based on Attribute-based Credentials that consists of a list of attribute-value pairs certified cryptographically by an issuer. The basic operation on Privacy-ABC credentials are the same as the X-509 certificates. But the realization of the Privacy-ABC is based on different cryptographic primitives, such as pseudonym systems(Chaum, 1981), anonymous credentials(Camenisch and Lysyanskaya, 2001), self-blindable credentials(Verheul, 2001), and minimal disclosure tokens(Brands, 2000).

Two projects founded in EU worked on identity management using Privacy-ABC technologies. The research project Privacy and Identity Management for Europe (PRIME) is a system for privacy-enhancing identity management that combines anonymous credentials with attribute-based access control, and anonymous communication. Ardagna et al. (2008) and Ardagna, Camenisch, Kohlweiss, Leenes, Neven, Priem, Samarati, Sommer and Verdicchio (2010) presented works related to the project that allow individual prove the possession of condition to satisfy the restrictions imposed by services on attributes without revealing personal information. The concepts of project achieved little practical applications in real world, because areas of user interfaces, policy languages, and infrastructure needed further research (Ardagna, De Capitani di Vimercati, Neven, Paraboschi, Preiss, Samarati, Verdicchio et al., 2010; Bichsel et al., 2013). Between 2008 and 2011 the work continued in the project Privacy and Identity Management in Europe for Life (PRIMELife) que tinha por objetivo apresentar soluções in identity management, integrating access control policy with privacy-preserving data handling policies. Ardagna, De Capitani di Vimercati, Neven, Paraboschi, Preiss, Samarati, Verdicchio et al. (2010) apresentou uma solução de controle de acesso baseado também em certificados de atributos mas usando padrões de mercado, no caso XACML (Rissanen, 2013) e SAML (Ragouzis et al., 2008). O primeiro, para autorização baseada em atributos, enquanto o segundo como um meio de transporte de declarações sobre fatos de autenticação e/ou autorização. No artigo o autor somente apresentou o modelo, não incluindo testes de validação de um possível protótipo, considering that the implementation was occurring in PRIMELife project. The projects PRIME and PrimeLife and the related works demonstrated the difficulty to applied the technologies to the production environments Bichsel et al. (2013).

The Privacy-ABC has two instantiating technologies that received commercial support. They are the IBM Identity Mixer (IDEMIX)(Camenisch and Van Herreweghen, 2002) that is based on the scheme proposed by Camenisch and Lysyanskaya (2001) and the Microsoft U-Prove, specification defined by Brands (2000). The core features of those technologies are: pseudonymity, the selective and minimal disclosure of attributes, untraceable of user authentications and unlinkability between of the revealed data by service providers. To use in online services the credential is transformed in a presentation token, that can be verified cryptographically. Another application of Privacy-ABC are electronic credentials based on smart cards exemplified by the project IRMA (I Reveal My Attributes)(Koning et al., 2014). A project known Attribute-based Credentials for Trust (ABC4Trust) founded by EU has the goal to address the federation and interchangeability of technologies related to Privacy-ABC. The establishment of the project reflects the difficulty of applicability of the technology in real world systems. The drawback of Privacy-ABCs technologies are the relative complexity (Nogueira, 2014) of the infrastructure needed for emission, verification and revocation of tokens and certificates. The slow adoption was caused mainly by the difficulty of use the technology (Camenisch et al., 2012). Another question is the assumption of a central authority (Bertino and Takahashi, 2011). As a technology based on public-key infrastructure the revocation of certificates are a harder problem to be solved. Compared to our proposal, one difference is the approach of privacy issue attacked by the system: we consider the identity provider trustworthy while the Privacy-ABC considerer that online identity provider can't be trusted. Furthermore they not address the RESTful services, fine-grained authorization based on XACML and user attributes given by an identity providers OAuth-based.

Kounga, Mont and Bramhall (2010) também seguiu a linha de estender o XACML, mas definindo uma autoridade que armazenasse os atributos e políticas. A proposta de Kounga em Kounga, Mont and Bramhall (2010) aborda a possibilidade de que o consentimento do usuário pode se estender tanto nas preferências de privacidade das informações pessoais quanto em dados. Além disso, através da extensão do XACML o consentimento pode ser de granularidade mais fina sobre os dados. Para evitar que os pontos PDP e PEP do XACML não tenham acesso às preferências de privacidade e de dados do usuário a arquitetura foi estendida para incluir módulos que tratam exclusivamente dos dados de atributos, que foi definido como *Attribute Authority* (AA). Apesar de apresentar a característica de autorização com privacidade, a solução necessita que uma autoridade de confiança (chamada de *data collector*) gerencie as preferências e os dados pessoais. Além disso, o artigo não apresentou uma implementação da proposta, em parte, devido ao fato da solução usar alguns conceitos e estender o framework do projeto *Identity Governance Framework* (IGF). A extensão do XACML para acomodar controle de acesso baseado em certificados de

atributos foi explorada pelos trabalhos de Camenisch et al. (2009) e Dagdee and Vijaywargiya (2011), o primeiro na forma de uma linguagem e outro na extensão da arquitetura.

Chadwick and Fatema (2012) propôs uma arquitetura em que fornece serviço de autorização para ambiente em cloud. A questão de privacidade é tratada sob dois aspectos: primeiro, através de diferentes PDPs que avaliam cada qual uma linguagem de política de privacidade diferente; e o conceito de *sticky policy*, que permite que os dados trafeguem entre instalações de nuvens mas mantendo presa a política de privacidade. O pressuposto adotado no trabalho foi que os provedores de serviço na nuvem são confiáveis de tal forma que vão honrar as políticas de privacidade definidas nas sticky policies oriundas de outros provedores no mesmo ambiente de nuvem. Trata-se de proposta dentro do projeto PERMIS Chadwick et al. (2008) that is framework to provide policy based authorisation for federated and/or grid applications using the standard SOAP/SAML protocol. The goal of the project is create a system with privacy preserving authorization and tools for management of policies. The architecture was defined and constructed over the SAML protocol and the entity that provide de user data was not specified by Chadwick and Fatema (2012) but PERMIS can be integrated with Shibboleth and Globus toolkit, while our proposal uses RESTful and OpenID Connect. Although the user has control of his privacy PII, the model depends on the service provider respect the policy.

Architectures for policy decomposition Lin et al. (2008) and policy federation Decat, Lagaisse and Joosen (2012); Decat et al. (2013); Decat, Lagaisse and Joosen (2014) aimed to provide confidentiality and privacy when enforcing access control policies in distributed environment. The proposed works are supported by the XACML policy and architecture, because the entities are specified to be easy distributed. The proposed works are supported by SOAP/SAML protocols and the relationship with identity providers were not defined in their proposals.

The identity management consolidated the externalization of user authentication. The domain service that maintains the attributes and the identities are outside of the resource domain. An example of well know package for web single sign-on and for identity federation is the open source Shibboleth (Erdos and Cantor, 2002). It's based on OASIS Security Assertion Markup Language (SAML) and in Shibboleth version 2.0 the OpenSAML is the stack that provides the XML support. For the purposes of this work the Shibboleth don't or partially meets the requisites, because of this considerations: Shibboleth uses SAML and it is a SOAP/XML based protocol; the SAML infrastructure for federation needs explicit trust configuration; and the service providers based on SAML and Shibboleth are tightly coupled to the identity providers. Those characteristics difficult the adoption for a Web more light, based on RESTful Web API and desktop/mobile based. Another recent system for identity management is the OpenID Connect, which is defined as identity layer on OAuth 2.0. The main advantages are the use of RESTful Web APIs and JSON for transport the user assertions. However the two mentioned protocols don't have the aim to provide fine-grained authorization, only the authentication of user and transport of claims about it.

Externalization of authorization in Web applications took to the protocols OAuth and User-Managed Access (UMA)(Hardjono et al., 2016; Machulak et al., 2010). The OAuth 2.0 provides a mechanism to a user authorize third-party applications access his or her resources without expose private credentials. For that online services on behalf of user, the protocol uses access tokens as credentials. The flow of messages is based on JSON and the access through open APIs. The UMA protocol is a profile of OAuth 2.0 in that the user manages the policy of access control to his protected resources (personal data, content or services). This is achieved by the user defining the policies in a central authorization server (AS) and the requesting parties (RP) adhering to a set of obligations (Hardjono and Maler, 2015). Resuming, UMA is a protocol for authorization in Web 2.0 that leverage to the user of control about his data, that is, the UMA is user-centric while our proposal is centred in service but offering privacy about PII. Another difference is that the UMA needs agreement between authorization server and requesting party that possibilities the AS trust that the RP enforces the user defined policies while ours concept is that the RP is untrusted.

Werner et al. (2015) presented an approach and in Werner and Westphall (2016) a model for an identity management with privacy in cloud infrastructure. The model comprises a IdM in cloud where SP and IdP in work together through interactions to permit users consume services in a environment with the next characteristics: user receiving trust information based on reputation and risk analysis of SP, minimization of release of personal attributes, obfuscation of user activities through anonymity and pseudonyms, and the possibility of user defining the privacy policy related to the disclose of data to the cloud. Even though the authors presented a model with attempt to help users in making decision about her or his privacy, the architecture depends on the SP enforce the privacy policy. Concerning the PII, our proposal permits the user access services protected by fine-grained policies and without releasing information about certain attributes.

O trabalho de Ma and Sartipi (2015) apresentou um modelo em que os usuários eram identificados por uma federação *OpenID Connect* e o controle de acesso através do XACML. Para incluir o consentimento dos usuários sobre a liberação de seus dados, foi criado um servidor de políticas XACML ligado ao servidor de identidade. O mérito da proposta é a inclusão de um servidor de políticas XACML ligado ao servidor de identidade *OpenID Connect*. Essa solução permitiu descrever os escopos e atributos mais complexos em

termos de linguagem de controle de acesso do XACML. Apesar de usar padrões atuais, a solução de Ma foi adaptada especificamente para resolver a questão do acesso de pacientes, médicos e colaboradores sobre os dados de imagens de diagnóstico médico disponibilizados por diferentes clínicas e hospitais dentro de uma nuvem.

3 Background and Context

This section discusses the main topics that are related to the context of this work. Specifically, access control, identity management and privacy.

The access control is the centre of security of any information system asset and resides in all levels, from hardware to application (Anderson, 2008). The main goal of access control is mediate requests to resources and enforce the decision of grant or deny (Samarati and Di Vimercati, 2001). But, as denoted by Gollmann (2011), the process of controlling access is evaluated in two steps: authentication and authorization. The authentication is the mechanisms that verifies with trustworthy the identity of the entity that is requesting access to resources. Authorization is the process of regulating the access control. With the complexity of interactions between consumer and provider of services and the increasing of online services took the outsource of the procedures of authenticate and authorize users and applications. Our work has based on those protocols and systems.

Sistemas de controle de acesso baseados em identidade assumem que a autenticação foi realizada e o principal foi identificado com sucesso. Os três sistemas clássicos de ampla adoção e que são baseados no princípio mencionado são: the Discretionary Access Control (DAC); the Mandatory Access Control (MAC); e o mais recente, the Role Based Access Control (RBAC). O controle de acesso discricionário Lampson (1974) se baseia em uma matriz de acesso constituída de domínios de proteção (usuários e objetos) cuja principal característica é o fato deste modelo delegar a política de segurança para o usuário, ou seja, as entidades controlam quem e como pode realizar determinado acesso. O modelo que foi proposto a seguir foi o Role-Based Access Control (RBAC), que foi formalizado por Ferraiolo and Kuhn (1992) e cuja principal motivação foi atender ao estabelecimento de políticas de controle de acesso em ambientes corporativos. A característica principal deste modelo é a separação da ligação direta entre os usuários e as respectivas permissões. Aos papeis são associados conjuntos de permissões que regulam as operações sobre os objetos.

A evolução da computação trouxe questões que modelos tradicionais de controle de acesso baseados em identidade já não podiam satisfazer. As mais importantes foram: o usuário já não está mais definido; a computação agora é realizada tanto no servidor quanto no cliente; políticas de controle de acesso evoluíram para considerar aspectos tanto do sujeito quanto do objeto e questões ambientais relativas às operações. Essa e outras necessidades levaram à formalização of model Attribute Based Access Control (ABAC), definido formalmente em Hu et al. (2014): o controle de acesso aos objetos é obtido pela avaliação de regras considerando os atributos das entidades (sujeito e objeto), das operações e do ambiente, relevantes para a requisição. O modelo conta com várias entidades, que realizam diferente funções, permitindo a implementação distribuídos desses unidades.

The entities that compose the ABAC were first defined in the Recommendation X.812 da ITU-T, de 1995 (*ITU-T Recommendation X.812 (1995)—ISO/IEC 10181-3:1996, Information Technology - Open Systems Interconnection - Security frameworks in Open Systems: Access control framework*, 1996) and each point has specific function. The Policy Decision Point (PDP): avalia a política aplicável à requisição que resulta em uma decisão de autorização, que é retornada para a entidade responsável por cumprir a política. The Policy Enforcement Point (PEP) is the entity efetivamente realiza o controle de acesso, protegendo o recurso. Recebe as requisições de acesso e as envia para o PDP for evaluation and cujas respostas de autorização definem o cumprimento da política. The policy are created and maintained by the Policy Administration Point (PAP). An important entity in the ABAC model is the Policy Information Point (PIP), which serve como repositório e origem para os atributos necessários à avaliação da política.

Ao lado das muitas vantagens, há alguns problemas, dois dos quais serão apresentados pela sua importância: o primeiro é que todos os participantes na autorização ABAC devem concordar com o significado dos atributos (Karp, Haury and Davis, 2010; Rubio-Medrano et al., 2015) e também há necessidade de definir os atributos relevantes para o controle de acesso; e, em segundo lugar, the Policy Enforcement of Policy devem ser implementados em todos os recursos que deverão ser protegidos pelo ABAC.

The Organization for the Advancement of Structured Information Standards (OASIS) defined the standard eXtensible Access Control Markup Language (XACML)Rissanen (2013) based on the advantage of ABAC for fine-grained authorization. The XACML describes the core parts: a policy language express in XML; a request-response protocol and a reference architecture. The decoupled architecture is almost the same as specify in Hu et al. (2014) and *ITU-T Recommendation X.812 (1995)—ISO/IEC 10181-3:1996, Information Technology - Open Systems Interconnection - Security frameworks in Open Systems: Access control framework* (1996) but with the inclusion of Context Handler, that mediates the communication between the components.

The language of XACML define the policy that the architecture needs to evaluate and enforce. The top-level policy elements are *PolicySet*, *Policy*, and *Rule*. The PolicySet contains set of PolicySet and set of Policies. The Policy in turn contains one or more

Rule elements and as such is the elementary unit of evaluation of the policy by the PDP. The Rule has three main parts: Target which denotes rule's applicability to the authorization request, Conditions which are authorization predicates over attributes, and Effect is the result of the rule evaluation. It returns either "Permit" or "Deny" if the rule is satisfied and "Non Applicable" if the Target and/or Conditions are not satisfied. The Policy returns "Indeterminate" when the PDP is unable to evaluate the request, by error or by missing attributes. The Target element can be included in all the top-level elements (PolicySet, Policy, and Rule) and it cat be considered as an applicability filter on subject, resource, action and environment attributes. The Target element of Policy index the policies and it permits the PDP to determine the applicable policy for the request. The Obligation and Advice expressions are returned with the decision to the PEP and they inform the actions that the enforcement point need take along with the decision of request. The difference between them is that the Advice element may be safely ignored by PEP. When there are multiples Rule elements with each one resulting in a decision and when there are more than one Policy elements in a PolicySet container, there are a mechanisms that decide the final outcome of Rule/Policy evaluation. For that, the PolicySet defines a *policy combining algorithm* and a *Policy* defines a *rule combining algorithm*. Examples of those algorithms are: deny-overrides, permit-overrides, first-applicable.

A avaliação de uma política pelo PDP funciona da seguinte forma: ponto de avaliação verifica se correspondências definidas pela *Target* são satisfeitas pelos atributos na requisição. Portanto, uma decisão de acesso é baseada nos atributos do sujeito, objeto, ambiente e nas operações matemáticas sobre os mesmos, os quais definem os predicados de autorização.

A especificação XACML está em sua versão 3.0, lançada em 22 de janeiro de 2013, e conta com um conjunto de profiles que permitem acrescentar características à especificação padrão. Alguns profiles: política de privacidade (XACML v3.0 Privacy Policy); SAML; profile para o modelo de controle de acesso baseado em papeis (XACML v3.0 Core and Hierarchical Role Based Access Control (RBAC) Profile Version 1.0). For this work, the profile of REST and JSON are important to permit the architecture be used in RESTful environment with the OpenID Connect.

3.1 Identity Management

Identidade completa de um indivíduo é o conjunto de identidades parciais que representam a pessoa num determinado contexto as quais são caracterizadas por um subconjunto de valores de atributos Pfitzmann and Hansen (2010). Para minimizar a necessidade de cadastro das informações pessoais em cada provedor de serviço, surgiram os sistemas de gerenciamento de identidade El Maliki and Seigneur (2007) Cao and Yang (2010). The main objective is securely transport attributes of identities between parties in different domains that permits users realize authentication via Single Sign On (SSO). And as defined by Bertino and Takahashi (2011), the Identity Management (IdM) has the responsibility of maintain the integrity of the life cycle of identities, including the creation, use, update, and revocation.

When the entities related to Identity Management cooperates to achieve a common result we have a Federated Identity Management (FIM). The federation define and regulate the relationship between identity providers and service providers to create a single virtual domain (Perez-Mendez et al., 2014) (Cao and Yang, 2010). Specifically, the federated model must have a set of agreements, standards and technologies that permits service providers recognize and trust the identities of users provided by the IdP (Torres, Nogueira and Pujolle, 2013).

Os padrões que são usados para criar sistemas de gerenciamento de identidade e federações de identidade na *Web* são: SAML, OAuth, OpenID, OpenID Connect e especificações WS-*. O padrão Security Assertion Markup Language (SAML) Ragouzis et al. (2008), define declarações de autenticação e autorização em linguagem XML e também os protocolos de transporte dessas declarações. Vários sistemas de federações de identidade são baseadas no SAML, dos quais vale destacar o Shibboleth Erdos and Cantor (2002) e SimpleSALMLphp. Os protocolos OpenIDopenid (2005) e OAuthHardt (2012) são baseados em HTTP e são usados respectivamente para autenticação e autorização de usuários sem a necessidade de divulgar credenciais (principalmente senhas) para os provedores de serviço. O OpenID foi originalmente especificado para prover autenticação enquanto que o OAuth foi criado para delegar autorização, entre SP e IdP. O OpenID Connect v. 1.0 Sakimura et al. (2014) é um procolo que estabeleceu uma camada de identidade federativa sobre o protocolo OAuth 2.0, que permite criar federações de identidade usando mensagens REST, resultando em clientes que podem ser executados tanto sobre navegadores quanto sobre dispositivos móveis. *WS-Federation* Goodner and Nadalin (2009) é uma especificação criada pela OASIS e indústria (IBM e Microsoft) e que define os mecanismos para criar federações de identidade usando XML, mensagens SOAP e Web Services Description Language (WSDL). Ela está suportada nos padrões OASIS WS-Security e WS-Trust.

3.2 Privacy

A privacidade é um conceito amplamente divulgado mas que não possui uma definição única. Para este trabalho será adotado os autores Pfitzmann and Hansen (2010) propõem ampla conceituação envolvendo esse tema. Primeiramente, privacidade é o direito de indivíduos, grupos ou instituições de determinar quando, como e qual informação sobre os mesmos é comunicada aos outros. Ainda, traz o importante conceito de

minimização de dados, o qual resumidamente é diminuir a possibilidade, a quantidade e o tempo sob guarda de dados pessoais por terceiros. According to Pfitzmann and Hansen (2010) and Deng et al. (2011), privacy has been characterized by the next concepts. Anonymous is concerned to the subject that cannot be identified in the respective set. Unlinkability is the property that items (attributes or actions) of subject cannot be associated between them and/or with a subject. Undetectability is the capacity of a system to obfuscate attributes and actions related do the subject.

Uma linha importante que estende sistemas de controle de acesso para prover privacidade é a inclusão do atributo purpose que representa a finalidade para determinado acesso (ou para qual fim uma informação é usada) e que deve ser determinado pelo sistema antes da respectiva requisição. O texto de Byun, Bertino and Li (2005) apresenta um modelo de controle de acesso baseado numa extensão do RBAC que incorpora atributos com propósito nos papeis e papeis condicionais.

The user privacy has received support of law and norms whose purpose is mediate the data usage and privacy of personal data. Legal context concerning data protection and privacy promoted by governments began in 1973, in Sweden, and in 1974, in US. Privacy is also acknowledged as a fundamental human right by the Universal Declaration of Human Rights of the United Nations in 1974. The Organisation for Economic Cooperation and Development (OECD) provided in 1980 the first guidelines to protect privacy based on national consensus. The guidelines consist of eight basic privacy principles that was revised in 2013 and with the EU's Data Protection Directive 95/46/EC influenced worldwide laws and frameworks.

4 Example Scenario

In this section we will illustrate the problem and the proposed solution through a sample scenario. The example refers to a public library (PubLib) that permits borrowing materials like books and digital media to a citizens that have been registered in an public organization (PubOrgIdP) that supports an identity provider. The library don't want maintain system and/or database of the users profile.

The library wants use authorization based on attributes and externalized of the application. Architecture should be implemented as RESTful services, with the following constraints: a) services need to communicate in JSON; b) services need to be stateless; c) use of service by desktop/mobile platforms. The solution that permits comply with the requirements is the XACML 3.0, because is modular, have included the REST/JSON profiles and the policy of use of service can be enforce by specifying the rules in the language. The organization that offers service of identity provider wants an application that permits users to register, control and releases via consent their personal data over a RESTful architecture. Was chosen the OpenID Connect that is a recent specification and has several open source implementations.

The service of borrow materials has subject to follow policies:

P1 Anyone can search materials on PubLib;

P2 Any material (physical or digital) only can be booking and borrow to citizen that authenticates to PubOrgIdP;

P2 The user authentication with identification or by pseudonym;

P3 The library borrows up until tree materials;

P4 If a user is older than 60 years and lives in the same region of the library, then the materials can be shipping free of charge;

P5

4.1 Problem Statement and Solution

Scenario The Scenario dimension defines the primary untrusted actor and potential attacker in a privacy-sensitive information exchange operation.

The Untrusted Server scenario describes the case of a service provider that aims to gain more information about the service consumers than necessary. This usually relates to the identity of the service consumers, leading to techniques such as anonymous communication which can be realized by relying on intermediate proxies between a sender and a receiver responsible for masking the sender's identity (cf. (Chaum,1981)). The main issue with anonymous communication is

Proposed scope

When modelling a privacy-enhancing technologies (PET) technical measure we needs define the scope and the aims of the work. Considering the OECD guidelines (Organization for Economic Co-Operation and Development, 2013), the model deals with the principle of Collection Limitation in that the user can use the service provider without presenting the value of his attribute relating to personal data. The main idea is protect the personal information in the state of data at rest (Liu and Kuhn, 2010), not treating with the attribute that the user release to service provider, in instance, data in motion, that requires different technical solution.

The principal goal of the model presented in this paper is that which aim at preserving the privacy of individuals or groups of individuals. Numerous PETs have been A proposta deste projeto considera alguns pontos que são pressupostos ou que não fazem parte do modelo, mas podem interagir quanto a aspectos de segurança. Os principais pontos a serem considerados na proposta:

1. Considerando a taxonomia apresentada por Heurix em Heurix et al. (2015), os alvos de tecnologias of Privacy-Enhancing Technologies (PET) são a identidade, conteúdo e comportamento. No presente trabalho somente o aspecto da identidade será considerado para fins de manutenção da privacidade do usuário.
2. Durante a liberação de política do provedor de serviço para o provedor de identidade, podem surgir questões de privacidade. Para contornar essa questão, a proposta prevê que somente a política restrita à avaliação dos atributos do usuário sejam enviados para o IdP.
3. Extensões ao protocolo OAuth 2.0 e à especificação XACML deverão ser incluídas para comportar a proposta do modelo.

While privacy usually refers to protecting the identity of the persons involved, Content refers to the data processed or created during the service consumption, including both payload as well as meta data. (Heurix et al., 2015) Considering of aspect of privacy preserving, the model deals with the principle of Collection Limitation (Organization for Economic Co-Operation and Development, 2013) and treats of data-at-rest (Liu and Kuhn, 2010)

5 Proposed Model

A proposta a ser desenvolvida no decorrer do período da pesquisa será apresentada a seguir considerando os principais aspectos que deverão ser modelados nas especificações e sistemas em uso. Antes da exposição, serão apresentadas as restrições que escopos que nortearão a construção da proposta, alguns dos quais já informados nos objetivos.

5.1 XACML

5.2 OAuth 2.0 and OpenID Connect

The OAuth 2.0 is a protocol for authorizing applications on behalf of users

O OpenID Connect (OIDC) consiste de uma camada de identidade sobre o protocolo OAuth 2.0 para prover gerenciamento de identidade sobre arquitetura RESTful. It is used to provide the function of authentication and the transport of claims about the user to the resource server. o *OpenID Connect* é uma especificação muito recente, de fevereiro de 2014.

Simple identity layer on top of OAuth 2.0 Enables clients to verify identity of end-user Enables clients to obtain basic profile info REST/JSON interfaces low barrier to entry: Designed to work well on mobile phones

UserInfo endpoint for simple claims about user

Na figura fig-openidconnect-fluxomensagens são apresentados os fluxos de mensagens entre as três seguintes entidades:

1. Relaying Party (RP): entidade que requer a autenticação e afirmações do usuário final a partir do provedor de identidade OpenID Connect. A nomenclatura segue o estabelecido no protocolo OAuth 2.0, no qual essa entidade recebe o nome de cliente.
2. OpenID Provider (OP): é a entidade capaz de autenticar o usuário final e prover afirmativas sobre o mesmo para o RP. No protocolo OAuth 2.0 é denominado de servidor de autorização (OAuth 2.0 *Authorization Server*).
3. End-User: é o usuário final, ou seja, é o ser humano participante do protocolo.

FIGURA: fluxo mensagens OpenID Connect

Basicamente, o fluxo de mensagens seguem os seguintes passos:

1. The RP (Client) envia uma requisição de autenticação para o OP (OpenID *Provider*).
2. O OP autentica (AuthN) o usuário final e obtém autorização (AuthZ).
3. O OP responde com um Token de ID e usualmente com um Token de acesso (AuthN *response*).
4. O RP pode enviar a requisição contendo o Token de acesso para o ponto de informação sobre dados (atributos) do usuário (*UserInfo Endpoint*).
5. O ponto de informação (*UserInfo Endpoint*) retorna *claims* sobre o usuário final.

Sobre o fluxo, há algumas considerações. As mensagens iniciam com o usuário fazendo uma requisição de acesso a uma aplicação no lado do RP. As mensagens (1), (3), (4) e (5), no fluxo padrão, são redirecionadas através do usuário, geralmente via navegador *Web*.

6 Definição da proposta

A proposta para acomodar os objetivos deste trabalho prevê a inclusão de uma implementação do XACML in the service provider (Relaying Party - RP) e modificações em uma implementação do *OpenID Connect* (OP). Na figura **??** há apresentação do esquema geral do *OpenID Connect*, mostrando os fluxos de dados básicos. Na mesma figura, à direita, as modificações e inclusões que permitem o modelo realizar a avaliação das políticas de acesso no IdP, de forma que atributos já não serão transmitidos para o provedor de serviço, resultando na obtenção da privacidade objetivo da proposta.

FIGURA: proposta

Funcionamento da proposta:

1. As políticas do XACML ficam armazenadas no ponto de administração de políticas (PAP) e ficam disponíveis para o PDP para fins de avaliação da requisição.

2. O usuário faz uma requisição ao provedor de serviço, que é interceptado pelo módulo PEP do XACML.

3. O XACML deverá ser estendido através de modificações no módulo do PDP para fazer uma pré-avaliação da política mais adequada e a seguir extrair a avaliação referente aos atributos do usuário.

4. Através de extensão ao protocolo OAuth 2.0 (usado pelo *OpenID Connect* para realizar toda a comunicação), uma solicitação de avaliação junto com a política é enviada ao *OpenID Connect* (módulo *UserInfo Endpoint*).

5. A requisição de avaliação é interceptada e encaminhada ao módulo do PDP a ser incluído na implementação do *OpenID Connect*.

6. O resultado da avaliação é retornado para o provedor de serviço (XACML) que sujeitará a requisição original ao restante da avaliação de atributos (do recurso e de ambiente) e condições. O restante do protocolo permance inalterado.

The policy needs to be passed dynamically along with the decision request to the authorisation service so that the data subject, or the application acting on her behalf, does not need to access the PAP for storing the policy prior to the authorisation decision. The chosen protocol should be able to pass policies in any policy language (assumption 1 of Section 3.2) along with the request context. This step is the same as proposed by Chadwick and Fatema (2012) Fatema (2013)

7 Resultados esperados

Para validar o modelo de autorização, mantendo a privacidade, será estabelecido um caso de uso, no qual serão criadas políticas de controle de acesso que atendam a maior parte dos requisitos. Como a avaliação de políticas pelos pontos de avaliação (PDP) já estão bem definidos, espera-se que a proposta possa ser validada sem problemas.

Em termos de desempenho, não há um trabalho relacionado que possa servir de parâmetro para quantificar o custo relativo da proposta. Mas, considerando que há necessidade de estender dois protocolos e incluir mais código de transporte, comunicação e avaliação de política, o desempenho tende a diminuir, aumentando a latência das decisões. Há duas questões que surgem para diminuir o impacto: a primeira seria a otimização, tanto dos códigos quanto das transações, isso após validar quanto à correção; a segunda, é considerar que essa proposta se destina a operações de controle de acesso que demandam intervenção humana na questão do consentimento, o que pode minorar a expectativa de latência nas respostas. O maior impacto poderia ocorrer no provedor de serviço, que poderia adotar soluções como otimização de avaliação de políticas de XACML Mourad and Jebbaoui (2014) e distribuição dos processos num ambiente paralelo.

8 Validation of model

9 Conclusions

This paper presents a new approach to realize fine-grained access control in environment with a identity provider OpenID Connect supplying PII data. The user controls the releasing the personal information. By adopting the evaluation of the service policies in the same domain of the identity provider, the personal data do not needs to be transported to the service provider. As a result of this, the privacy of PII is obtained and the user do not need care of the potential use of personal data by service providers. Important characteristic of this schema is the usability, because the user not need to established privacy policies concerning of manipulating his data. Future works go in direction of research the monitoring and auditing of privacy protection provided by the IdP and on the other side there is the question of decomposition of policy and include this in the model presents in this paper.

Acknowledgements

The authors would like to acknowledge the support from the LRG-UFSC.

References

Anderson, Ross. 2008. *Security engineering*. John Wiley & Sons.

Ardagna, Claudio Agostino, Jan Camenisch, Markulf Kohlweiss, Ronald Leenes, Gregory Neven, Bart Priem, Pierangela Samarati, Dieter Sommer and Mario Verdicchio. 2010. "Exploiting cryptography for privacy-enhanced access control: A result of the PRIME Project." *Journal of Computer Security* 18(1):123–160.

Ardagna, Claudio Agostino, Marco Cremonini, S De Capitani di Vimercati and Pierangela Samarati. 2008. "A privacy-aware access control system." *Journal of Computer Security* 16(4):369–397.

Ardagna, Claudio Agostino, Sabrina De Capitani di Vimercati, Gregory Neven, Stefano Paraboschi, Franz-Stefan Preiss, Pierangela Samarati, Mario Verdicchio et al. 2010. Enabling privacy-preserving credential-based access control with XACML and SAML. In *Computer and Information Technology (CIT), 2010*

IEEE 10th International Conference on. IEEE pp. 1090–1095.

Bertino, Elisa and Kenji Takahashi. 2011. *Identity Management: Concepts, Technologies, and Systems*. Artech House.

Bichsel, Patrik, Jan Camenisch, Maria Dubovitskaya, Robert R Enderlein, Ioannis Krontiris, Anja Lehmann, Gregory Neven, Janus Dam Nielsen, Christian Paquin, Franz-Stefan Preiss et al. 2013. "H2.2 - ABC4Trust Architecture for Developers." *ABC4Trust heartbeat H* 2:2. [online] `https://abc4trust.eu/download/ABC4Trust-H2.2_ABC4Trust_Architecture_for_Developers.pdf` (Accessed 13 November 2015).
URL: *https://abc4trust.eu/download/ABC4Trust-H2.2_ABC4Trust_Architecture_for_Developers.pdf*

Brands, Stefan A. 2000. *Rethinking public key infrastructures and digital certificates: building in privacy*. MIT Press.

Byun, Ji-Won, Elisa Bertino and Ninghui Li. 2005. Purpose based access control of complex data for privacy protection. In *Proceedings of the tenth ACM symposium on Access control models and technologies*. ACM pp. 102–110.

Camenisch, Jan and Anna Lysyanskaya. 2001. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In *Advances in CryptologyEUROCRYPT 2001*. Springer pp. 93–118.

Camenisch, Jan and Els Van Herreweghen. 2002. Design and implementation of the idemix anonymous credential system. In *Proceedings of the 9th ACM conference on Computer and communications security*. ACM pp. 21–30.

Camenisch, Jan, Maria Dubovitskaya, Anja Lehmann, Gregory Neven, Christian Paquin and Franz-Stefan Preiss. 2012. A language framework for privacy-preserving attribute-based authentication. Technical report Technical Report RZ3818, IBM.

Camenisch, Jan, Maria Dubovitskaya, Robert R Enderlein, Anja Lehmann, Gregory Neven, Christian Paquin and Franz-Stefan Preiss. 2014. "Concepts and languages for privacy-preserving attribute-based authentication." *Journal of Information Security and Applications* 19(1):25–44.

Camenisch, Jan, S Modersheim, Gregory Neven, S Preiss and Dieter Sommer. 2009. Credential-based access control extensions to xacml. In *W3C Workshop on Access Control Application Scenarios, Luxembourg*. Vol. 17.

Cao, Yuan and Lin Yang. 2010. A survey of identity management technology. In *Information Theory and Information Security (ICITIS), 2010 IEEE International Conference on*. IEEE pp. 287–293.

Chadwick, David, Gansen Zhao, Sassa Otenko, Romain Laborde, Linying Su and Tuan Anh Nguyen. 2008. "PERMIS: a modular authorization infrastructure." *Concurrency and Computation: Practice and Experience* 20(11):1341–1357.

Chadwick, David W and Kaniz Fatema. 2012. "A privacy preserving authorisation system for the cloud." *Journal of Computer and System Sciences* 78(5):1359–1373.

Chaum, David L. 1981. "Untraceable electronic mail, return addresses, and digital pseudonyms." *Communications of the ACM* 24(2):84–90.

Dagdee, Nirmal and Ruchi Vijaywargiya. 2011. "Extending XACML to support Credential Based Hybrid Access Control." *IJCSI* .

Decat, Maarten, Bert Lagaisse, Dimitri Van Landuyt, Bruno Crispo and Wouter Joosen. 2013. Federated authorization for software-as-a-service applications. In *On the move to meaningful internet systems: OTM 2013 Conferences*. Springer pp. 342–359.

Decat, Maarten, Bert Lagaisse and Wouter Joosen. 2012. Toward efficient and confidentiality-aware federation of access control policies. In *Proceedings of the 7th Workshop on Middleware for Next Generation Internet Computing*. ACM p. 4.

Decat, Maarten, Bert Lagaisse and Wouter Joosen. 2014. "Middleware for efficient and confidentiality-aware federation of access control policies." *Journal of Internet Services and Applications* 5(1):1–15.
URL: *http://dx.doi.org/10.1186/1869-0238-5-1*

Deng, Mina, Kim Wuyts, Riccardo Scandariato, Bart Preneel and Wouter Joosen. 2011. "A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements." *Requirements Engineering* 16(1):3–32.

El Maliki, Tewfiq and Jean-Marc Seigneur. 2007. A survey of user-centric identity management technologies. In *Emerging Security Information, Systems, and Technologies, 2007. SecureWare 2007. The International Conference on*. IEEE pp. 12–17.

Erdos, Marlena and Scott Cantor. 2002. "Shibboleth architecture draft v05." *Internet2/MACE, May* 2:33.

EU Directive. 1995. "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 of the EC* 23(6). [online] `http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046` (Accessed 01 march 2016).
URL: *http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046*

Fatema, KANIZ. 2013. Adding Privacy Protection to Policy Based Authorisation Systems PhD thesis PhD thesis, University of Kent, UK (to appear, 2014).

Ferraiolo, David F. and D. Richard Kuhn. 1992. Role-based access controls. In *Proceedings of 15th NIST-NCSC National Computer Security Conference*. Vol. 563 Baltimore, Maryland: NIST-NCSC.

Gollmann, Dieter. 2011. *Computer Security*. 3 ed. John Wiley & Sons.

Goodner, M and A Nadalin. 2009. "Web Services Federation Language (WS-Federation) Version 1.2.". [online] `http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html` (Accessed 25 October 2015).
URL: *http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html*

Gürses, Seda, Carmela Troncoso and Claudia Diaz. 2011. "Engineering privacy by design." *Computers, Privacy & Data Protection* 14.

Hardjono, Thomas and Eve Maler. 2015. Binding Obligations on User-Managed Access (UMA) Participants. Internet-Draft draft-maler-oauth-umatrust-03 Internet Engineering Task Force. Work in Progress.
URL: *https://tools.ietf.org/html/draft-maler-oauth-umatrust-03*

Hardjono, Thomas, Eve Maler, Maciej Machulak and Domenico Catalano. 2016. User-Managed Access (UMA) Profile of OAuth 2.0. Internet-Draft draft-hardjono-oauth-umacore-14 Internet Engineering Task Force. Work in Progress.
URL: *https://tools.ietf.org/html/draft-hardjono-oauth-umacore-14*

Hardt, Dick. 2012. "The OAuth 2.0 authorization framework (RFC 6749).". [online] `http://www.rfc-editor.org/info/rfc6749` (Accessed 20 October 2015).
URL: *http://www.rfc-editor.org/info/rfc6749*

Heurix, Johannes, Peter Zimmermann, Thomas Neubauer and Stefan Fenz. 2015. "A Taxonomy for Privacy Enhancing Technologies." *Computers & Security* .

Hu, Vincent C, David Ferraiolo, Rick Kuhn, Adam Schnitzer, Kenneth Sandlin, Robert Miller and Karen Scarfone. 2014. "Guide to attribute based access control (ABAC) definition and considerations." *NIST Special Publication* 800:162.

ITU-T Recommendation X.812 (1995)—ISO/IEC 10181-3:1996, Information Technology - Open Systems Interconnection - Security frameworks in Open Systems: Access control framework. 1996.

Karp, Alan H, Harry Haury and Michael H Davis. 2010. From ABAC to ZBAC: the evolution of access control models. In *Proceedings of the 5th International Conference on Information Warfare and Security, ed. EL Armistead*. pp. 202–211.

Kolter, Jan, Rolf Schillinger and Günther Pernul. 2007. A privacy-enhanced attribute-based access control system. In *Data and Applications Security XXI*. Springer pp. 129–143.

Koning, Merel, Paulan Korenhof, Gergely Alpár and Jaap-Henk Hoepman. 2014. The ABC of ABC-An Analysis of Attribute-Based Credentials in the Light of Data Protection, Privacy and Identity. In *Internet, Law & Politics : A decade of transformations*, ed. Joan Balcells Padullés. Huygens Editorial pp. 357–374.

Kounga, Gina, Marco Casassa Mont and Pete Bramhall. 2010. Extending XACML access control architecture for allowing preference-based authorisation. In *Trust, Privacy and Security in Digital Business*. Springer pp. 153–164.

Kuschewsky, Monika. 2014. "The new privacy guidelines of the OECD: what changes for businesses?" *Journal of European Competition Law & Practice* p. lpu015.

Lampson, Butler W. 1974. "Protection." *ACM SIGOPS Operating Systems Review* 8(1):18–24.

Landwehr, Carl, Dan Boneh, John C Mitchell, Steven M Bellovin, Susan Landau and Michael E Lesk. 2012. "Privacy and cybersecurity: The next 100 years." *Proceedings of the IEEE* 100(Special Centennial Issue):1659–1673.

Lin, Dan, Prathima Rao, Elisa Bertino, Ninghui Li and Jorge Lobo. 2008. Policy decomposition for collaborative access control. In *Proceedings of the 13th ACM symposium on Access control models and technologies*. ACM pp. 103–112.

Liu, Simon and Rick Kuhn. 2010. "Data loss prevention." *IT professional* 12(2):10–13.

Ma, Weina and Kamran Sartipi. 2015. Cloud-based Identity and Access Control for Diagnostic Imaging Systems. In *Proceedings of the International Conference on Security and Management (SAM)*. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp) p. 320.

Machulak, Maciej P, Eve L Maler, Domenico Catalano and Aad Van Moorsel. 2010. User-managed access to web resources. In *Proceedings of the 6th ACM workshop on Digital identity management*. ACM pp. 35–44.

Mondal, Mainack, Peter Druschel, Krishna P Gummadi and Alan Mislove. 2014. Beyond access control: Managing online privacy via exposure. In *Proceedings of the Workshop on Usable Security, USEC*. Vol. 14.

Mourad, Alain and Hussein Jebbaoui. 2014. Towards efficient evaluation of XACML policies. In *Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference on*. IEEE pp. 164–171.

Nogueira, Hendri. 2014. "Aprimoramento da privacidade em infraestruturas de chaves públicas centradas no usuário e baseadas em notários.".

openid. 2005. "The OpenID project.". [online] `http://openid.net/` (Accessed 25 October 2015).
URL: *http://openid.net/*

Organisation for Economic Co-operation and Development. 1981. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. OECD.

Organization for Economic Co-Operation and Development. 2013. "Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013).". [online] `http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf` (Accessed 10 February 2016).
URL: *http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf*

Perez-Mendez, Alejandro, Fernando Pereniguez-Garcia, Rafael Marin-Lopez, Gabriel Lopez-Millan and Josh Howlett. 2014. "Identity Federations Beyond the Web: A Survey." *Communications Surveys & Tutorials, IEEE* 16(4):2125–2141.

Pernul, Günther. 2009. "Access-eGov: Access to e-Government Services Employing Semantic Technologies.". [online] `http://www-wiwi.uni-regensburg.de/Forschung/Projekte/Access-eGov-15.html.en` (Accessed 03 November 2015).
URL: *http://www-wiwi.uni-regensburg.de/Forschung/Projekte/Access-eGov-15.html.en*

Pfitzmann, Andreas and Marit Hansen. 2010. "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management.".

Ragouzis, Nick, John Hughes, Rob Philpott, Eve Maler, Paul Madsen and Tom Scavo. 2008. "Security assertion markup language (saml) v2. 0 technical overview.". [online] `http://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf` (Accessed 25 October 2015).
URL: *http://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf*

Rissanen, Erik. 2013. "eXtensible access control markup language (XACML) version 3.0 OASIS standard.". [online] `http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html` (Accessed 23 October 2015).
URL: *http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html*

Rubio-Medrano, Carlos E., Ziming Zhao, Adam Doupe and Gail-Joon Ahn. 2015. Federated Access Management for Collaborative Network Environments: Framework and Case Study. In *Proceedings of the 20th ACM Symposium on Access Control Models and Technologies*. SACMAT '15 New York, NY, USA: ACM pp. 125–134.
URL: *http://doi.acm.org/10.1145/2752952.2752977*

Sakimura, N., J. Bradley, M. Jones, B. de Medeiros and C. Mortimore. 2014. "OpenID Connect Core 1.0 incorporating errata set 1.". [online] `http://openid.net/specs/openid-connect-core-1_0.html` (Accessed 28 October 2015).
URL: *http://openid.net/specs/openid-connect-core-1_0.html*

Samarati, Pierangela and Sabrina De Capitani Di Vimercati. 2001. "Access control: Policies, models, and mechanisms." *Lecture notes in computer science* pp. 137–196.

Torres, Juana, Michele Nogueira and Guy Pujolle. 2013. "A survey on identity management for the future network." *Communications Surveys & Tutorials, IEEE* 15(2):787–802.

Verheul, Eric R. 2001. Self-blindable credential certificates from the Weil pairing. In *International Conference on the Theory and Application of Cryptology and Information Security*. Springer pp. 533–551.

Werner, Jorge, Carla Merkle Westphall, Rafael Weingartner, Guilherme Arthur Geronimo and Carlos Becker Westphall. 2015. An Approach to IdM with Privacy in the Cloud. In *Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on*. IEEE pp. 168–175.

Werner, Jorge and Carla Westphall. 2016. A Model for Identity Management with Privacy in the Cloud. In *2016 IEEE Symposium on Computers and Communication (ISCC) (ISCC2016)*. Messina, Italy: pp. 494 – 499.