Login Universal e Identidade na Web

Relatório do Trabalho Final de Curso

Licenciatura em Engenharia Informática

Orientador: José Guerreiro Faísca

Alunos: Basílio Mané Nº 20097598

Ulamam Mendes Dias Nº 20097241

Lisboa 2013

Agradecimentos

Agradecemos todo o amor, carinho e apoio que os nossos familiares nos deram desde sempre, principalmente nos momentos mais complicados e, que estivemos ausentes em suas vidas para finalizarmos este trabalho.

Os nossos agradecimentos aos Professores do Curso de Engenharia Informática da Universidade Lusófona de Lisboa (ULHT), sem esquecer dos professores da Universidade Lusófona da Guiné (ULG) que também deram as suas benéficas contribuições neste processo da formação;

De um modo geral, a todos os amigos e colegas, que através de sugestões, dúvidas e críticas que nos ajudarmos a clarificar e completar este trabalho, só podemos agradecer os momentos que passamos juntos, e que iremos continuar a passar.

Por último, gostávamos de agradecer em especial ao Prof. Mestre José Guerreiro Faísca pelos ensinamentos prestados, incentivo e sempre muita cordialidade.

Índice

Índice de Figuras

Resumo

Chegando a este ponto do percurso académico, e enquadrando na nossa área de interesses a escolha do projecto final recaiu sobre o estudo do protocolo WebID, uma solução de Login Universal e Identidade na Web.

O WebID, desenvolvido pelo W3C implementa uma infra-estrutura de autenticação. Trata-se de um protocolo de autenticação descentralizado, seguro, utilizando informações de perfil, bem como a camada de segurança SSL disponível nos browsers modernos.

O webID é uma forma de identificar uma pessoa, empresa, organização ou outro agente usando um URI (UniformResourceIdentifier).

Abstract

This work studies WebID, and implementation of a Universal Login and Identity on the Web. The WebID deploy an infrastructure-based authentication protocol and is developed by W3C.
It is a decentralized authentication protocol, secure, using profile information, as well as the layer of SSL security available in modern browsers.
The WebID is a way to identify a person, company, organization or other agent using a URI(Uniform Resource Identifier).

1-Introdução

Este trabalho tem como objectivo dar uma visão geral sobre o que é uma solução "Login Universal e Identidade na Web".

O WebID é uma maneira de identificar uma pessoa, empresa, organização ou outro agente usando um URI. O termo "WebID" foi cunhado por DanBrickley e Tim Berners-Lee, em 2000.

O protocolo WebID permite segurança e eficiência na autenticação de utilizadoresde modo amigável na web. Ele permite que os utilizadores se autentiquem em qualquer local, basta clicar sobre um dos certificados que lhes são propostas pelo seu browser. Estes certificados podem ser criadas por qualquer Web site para osseus utilizadores em um só clique. O identificador, conhecido como WebID , é um URI, cujo sentido pode encontrar-seno perfil associado a um utilizador (profile), um tipo de página web que qualquer utilizador de redes sociais está familiarizado.

Este WebID pode ser usado para construir uma rede de confiança usando vocabulários como FOAF (Friend-of-a-Friend) permitindo que os utilizadores liguemos seus perfis de forma pública ou protegida. Tal rede de confiança pode ser então utilizada por um serviço de forma a permitir o acesso a recursos, dependendo de propriedades do perfil como: ser conhecido por algumas pessoas relevantes, pertencer a uma determinada empresa, sermembro de uma famíliaou parte de algum grupo,

O protocolo WebID especifica como um serviço pode autenticar um utilizador depois de ter pedido o seu Certificado sem a necessidade de contar com o facto de este ser assinado por uma CA (Autoridade de Certificação) conhecida. O perfil WebID deve descrever o utilizador comosendo ele quem controla a chave privada relacionada com a chave pública publicado noCertificado utilizado para autenticar.

A autenticação WebID também pode ser usada para autenticação automática por robôs, como crawlersligados a repositórios de dados, que podem ser agentes que trabalham em nome dos utilizadores para ajudá-los nas suas tarefas diárias. O protocolo WebIDnão se limita a autenticação na Web, podendo trabalhar com qualquer protocolo baseado em TLS.

Conceitos

Representational State Transfer (REST) é um estilo arquitetural para construção de redes de informação distribuídos em larga escala, como a Web. Para construir tal rede énecessário que cada uma das peças utilizadas na construção seja capaz de crescer de forma independente de qualquer um dos outros, com muito pouca coordenação central, e em que cada um dos recursos assim criados poder referir-se facilmente a qualquer um dos outros. Os blocos lógicos para que isto funcione são as seguintes:

1. As especificações de nomes universais, também conhecido como Universal Resource Identifiers (URIs) | como os familiares Universal Resource Locator (URL).

2. O mapeamento de URIs de recursos, também conhecida como a relação de referência.

3. Métodos canónicos para manipular os recursos mapeados por cada URI, através de representações do recurso. Esse protocolo canônico apresentaum mecanismo que permite que o titular de uma URI consiga manipular o recurso referido por esse URI. Por exemplo, URLs, utilizando o protocolo HTTP como o seu mecanismo de referência: Ao enviar um GET solicitamos um determinado objecto URL, sendo retornada uma representação do recurso. Um recurso pode ser criado, alterado e excluído usando osmétodos POST, PUT e DELETE, respectivamente,

A Web Semântica

A Web semântica é uma extensão da Web atual, que permite aos computadores e humanos trabalharem em cooperação. A Web semântica interliga significados de palavras e, neste âmbito, tem como finalidade conseguir atribuir um significado (sentido) aos conteúdos publicados na Internet de modo que seja perceptível tanto pelo humano como pelo computador.

Na Web Semântica, torna-se possível utilizar URLs para se referir qualquer coisa, seja ele:

1. Coisas físicas por exemplo, pode referir-se https://romeo.example/#ium humano chamado Romeo;

2. Relações entre dois indivíduos por exemplo, a relação de saber<http://xmlns.com/foaf/0.1/knows> alguém conhece alguém;

3. Aulas por exemplo, as pessoas podem ser descritas como sendo casos de<http://xmlns.com/foaf/0.1/Person>, um conjunto de pessoas.

O significado desses URLs pode ser encontrado na referência,usando o seu protocolo canônico. Assim, fazendo uma requisição HTTP GET em<http://xmlns.com/foaf/0.1/knows>deve retornar uma representação. O HTTP é construído de modoa permitir a negociação de conteúdos.

Utilizando o URL acima num navegador Web, irá retornar umapágina HTML legívelque descreve a relação ‘conhece’. Um agente de Web Semântica poderia pedir arepresentação RDF padrão.

Um documento da Web Semântica é uma serialização de um gráfico que apresenta relações entre objetos. Cada relação existe como um triplo de <assunto><relações><objecto>, onde cada um dos sujeitos, relação e objecto pode ser escolhido dentro de qualquer um dos literais URI ou string.

FOAF, redes de reputação e da Web

FOAF, Friend-of.a-Friend (ou amigo-de-um-amigo), é um vocabulário RDF usado para descreverpessoas, agentes, grupos e suas relações. Quando usado na Web Semântica, isso permite que cada pessoa para descrever a si mesmo e a sua rede de amigos.

Ao dar-se o URI a um ID Web, pode-se descrever uma rede social pessoal, ligando-se a conhecidos por referência.

Assim, uma rede de informação pode ser construída, onde cada pessoaencarrega-se de manter atualizada a informação de que é responsável. À medida que a rede aumenta, o valor da rede aumenta exponencialmente, como definido pela Lei de Metcalf,, criando um círculo virtuoso. Sites de rede social actuais, como Facebook e LinkedIn, têm mostrado como isso pode funcionar em ambientes menos distribuídos, aproveitando-se da mesma lei.

O FOAF pode ser reforçada com descrições de confiança a fim de criar uma rede de reputação, e, no caso de FOAF + SSL, esta confiança pode realizar-se pelo uso de chaves criptográficas e de assinaturas, a fim de formar umaWeb segura(conforme descrito nas próximas seções).

Criptografia de chave pública

A Criptografia de chave pública permite que dois pares comuniquem de forma segura, sem que eles partilham um segredo, através da utilização de pares de chaves únicas. Uma chave, chamada de chave pública, pode ser amplamente divulgado, a chave privada, deve ser mantido apenas por seu dono. Isto está em contraste com a criptografia simétrica, onde ambos os participantes devem compartilhar o conhecimento da mesma chave secreta para criptografia e descriptografia.

Criptografia de chave pública baseia-se na suposição de que é inviável obter qualquer chave privada que corresponde a uma determinada chave pública através de força brutaporque esta operação é também computacionalmente dispendiosa. Ela também assume que dois indivíduos distintos irão gerar o mesmo par de chaves de forma aleatória.

Graças à dupla natureza do par de chaves pública e privada, duasações distintas são possíveis:

1. Criptografia é o obscurecimento de uma mensagem de texto simples, gerando uma mensagem encriptada utilizando a chave pública de um par de chave, de modo que só podem ser desencriptadosusando a chave privada correspondente.

2. Assinatura é o processo de associação de uma assinatura digital com uma mensagem, estaa assinatura é gerada utilizando a chave privada. De modo a permitir autenticidade e integridade, a mensagem pode ser verificada utilizando a chave pública correspondente.

A chave pública certificada é a combinação da assinatura por uma chave pública e algunsinformações relacionadas com esta chave. Tal certificado pode ser auto assinado (usando ochave privada que corresponde à chave pública que ele contém) ou assinado por uma terceira parte.

A parte que assina um certificado (auto assinado ou não) aprova o seu conteúdo.

Arquiteturastêm sido desenvolvidos para fazer uso deste modelo de chaves assimétricas: Caso do modelo hierárquico PKI (Public Key Infrastructure) ea cryptographic Web.

Em ambos os modelos são distribuídos certificados eos intermediários são confiáveis. Em ambos, o estabelecimento inicial de confiança (ou seja,a seleção de confiança) requer uma importação inicial de certificados. Mas esse processo é muito menos oneroso do que a obtenção de todas as chaves públicaspara todas as entidades que possam participar de comunicações seguras.

Infra-estrutura de chave pública (PKI)

A Internet X.509 Public Key Infrastructure(PKI) é um modelo hierárquico em quecertificados são assinados por uma Autoridade de Certificação (CA). O padrão X.509 incorporar um itemNome (Objecto DN), que identifica o objecto do certificado, e um item Emissor (Issuer DN), que identifica o emissor do certificado (entidade que assina o certificado). Um certificado X.509 só pode ter um DN Emissor, que deve ser o DN.Esta estrutura constrói uma árvore hierárquica da raiz CA certificada.

A maioria dos Web browsers e sistemas operativos fornecem uma lista padrão de CAs certificados que permite aos utilizador confiar implicitamente. Esta lista pode ser normalmentealterada pelo utilizador, um recurso frequentemente usado por PKI institucionais.

Autenticação SSL

O protocolo mais amplamente utilizado para proteger as comunicações entre um agente (cliente) e um servidor web é o Transport LayerSecurity (TLS) , ele próprio um sucessor do Secure Socket Layer 3.0 (SSLv3). O seu uso em aplicações de http é denotada pelo https em URLs.

Durante o reconhecimento SSL, no início da ligação, o cliente obtém um certificado X.509 do servidor. Neste ponto, o cliente verifica se o certificado é confiável,

Existe uma variante do processo, em que o cliente apresenta um certificado ao servidor, o que permite ao servidor autenticar o cliente usando o mesmo método.

De seguida descrevemos, do ponto de vista da Web Semântica, como a confiançanum certificado é avaliada. Isto constitui a base do FOAF + SSL.

Protocolo FOAF+SSL

O protocolo SSL + FOAF usa SSL e um modelo de Confiança PKI para verificar o certificado ao proteger um serviço. É importante a autenticação autorização. A autenticação é a ação de verificação da identidade do utilizador remoto. Autorização consiste em permitir ou negar o acesso ou operações a um determinado recurso, com base na identidade obtidos durante a autenticação.

O FOAF + SSL permite a um servidor autenticar um cliente dado uma URL simples.

Este URL pode ser usada diretamente para autorização, ou para explorar mais informações na web de dados vinculados, a fim de decidir se o referente da URL satisfazas restrições necessárias para acessoao recurso.

Sequência de protocolo

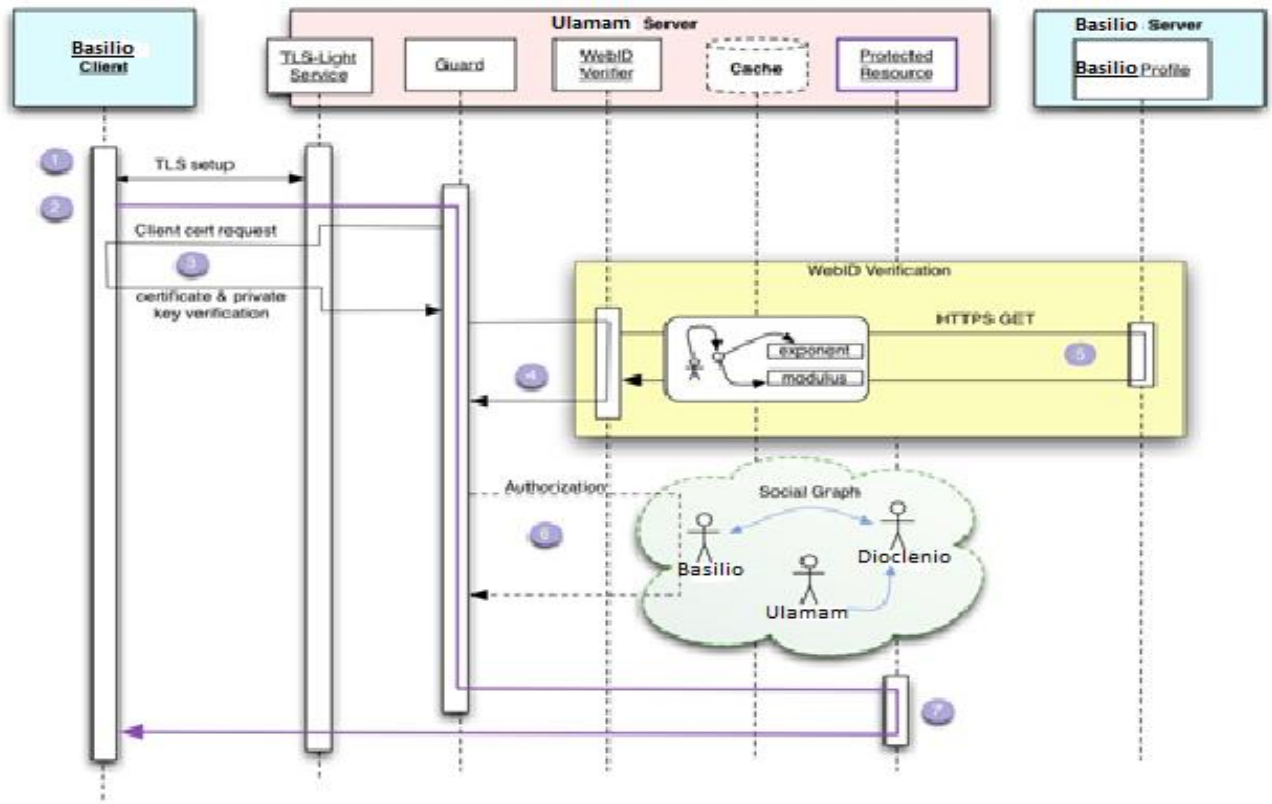

FIG. 1. O diagrama de sequência + SSL FOAF.

O protocolo de autenticação FOAF + SSL consiste nas seguintes etapas, conforme ilustrada na Figura 1:

1. Um cliente obtém um recurso HTTP público que aponta para um recurso protegido, por exemplo <https://juliet.example/location>.

2. O cliente, romeno dereferencia este URL.

3. Durante o "handshake" SSL, o servidor solicita o certificado do cliente. O FOAF + SSL não depende de nenhum CA. O valor do item "Alternative Name" do certificado X.509 contem o URI do cliente Romeo (https://romeo.example/#i) . Tal URI é conhecido como o WebID do utilizador.

Listing 1.1. Excerpt of a text representation of a FOAF+SSL certificate.

```
Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (1024 bit)
            Modulus (1024 bit):
                00:b6:bd:6c:e1:a5:ef:51:aa:a6:97:52:c6:af:2e:
                71:94:8a:b6:da:9e:5a:5f:08:6d:ba:75:48:d8:b8:
                [...]
            Exponent: 65537 (0x10001)
X509v3 extensions:
      X509v3 Subject Alternative Name:
                      URI:https://romeo.example/#i
```

FIG. 2.Extracto de uma representação de texto de um certificado foaf+SSL

Trabalho Relacionado

BrowserID

O BrowserID, é uma iniciativa recente (divulgado pela primeira vez em julho de 2011) de Identidade do Mozilla Team. Propõe a utilização de um endereço de E-mail como identificador único do utilizador, ao invés do URIs usado em Open ID e WebId. A alegação é que a maioria dos utilizadores de computador já estão confortáveis com o conceito de um endereço de E-mail que representa um indivíduo em particular, enquanto que poucas pessoas têm a mesma associação com URIs.

Além disso, muitas pessoas têm E-mails múltiplosque usam em diferentes contextos (comopara o trabalho, escola ou vida pessoal), da mesma forma, com o BrowserID, uma pessoa pode ter múltiplas identidades ou personas online simplesmenteusando diferentes endereços de e-mail. Este conceito aproveita novamente afamiliaridade e conforto que os utilizadores têm com endereços de e-mail.

Tecnologias e Ferramenta Utilizadas

Para o desenvolvimento desta Projecto, por uma questão de expectativas profissionais, resolvemo-nos pela utilização da tecnologia FOAF + SSL e integração com o site XWiki baseado no servidor Apache. O Apache é um software servidor HTTP desenvolvido pela Apache Software Foundation. É o mais popular servidor HTTP utilizado na imensa maioria dos servidores de hospedagem de sites. Um software livre com um tipo específico de licença, chamada licença Apache.

Análise de requisitos

Atendendo que, requisitos são as necessidades às quais o produto deve atender para resolver.

Atendendo ainda que requisito é um documento que contém a descrição precisa de cada funcionalidade e/ou necessidade para o sistema, na base disso tivemos atenção aos mesmos e na estruturação do referido projecto desde a fase de análise, da escolha dos programas, tecnologias, que finalmente utilizamos, a fim de evitarmos que haja controvérsia ou incompatibilidade durante a realização ou finalização do projecto.

Requisitos de Software e Hardware

Para o desenvolvimento deste projecto foram utilizados os seguintes requisitos de software:

- Apacheserver;
- Sistema Operativo: “Windows 7 Profissional”.
- Protocolo de autenticação FOAF + SSL e integração com o site XWiki

É também importante referir os requisitos de hardware utilizados para o desenvolvimento do mesmo:

- Um computador com arquitectura x86

É de salientar que todos estes requisitos foram muito importantes para a realização deste projecto.

Desenvolvimento do Projecto

A Web Social distribuída exige que cada pessoa seja capaz de controlar a sua identidade, que essa identidade passíveis de ligação entre os sites - colocando cada pessoa em uma teia de relações - e que seja possível autenticar globalmente com essas identidades. Ao realizar uma autenticação distribuída podemos proteger recursos e permitir configurações de privacidade preferenciais.

A especificação utilizada (WebID) descreve um mecanismo de identificação universal simples que é distribuído, abertamente extensível, com segurança, privacidade e controle sobre como cada pessoa pode identificar-se de forma a permitir o controle de acesso às suas informações na Internet. Ele faz isso através da utilização das melhores práticas de arquitetura Web, utilizandona sua construção protocolos e padrões amplamente utilizados bem estabelecidos, incluindo HTML, XHTML, URIs, HTTP, TLS, X509 e RDF Semântica.

As imagens seguintes mostram o processo de registo no siteXWiki e configuração do perfil do utilizador.

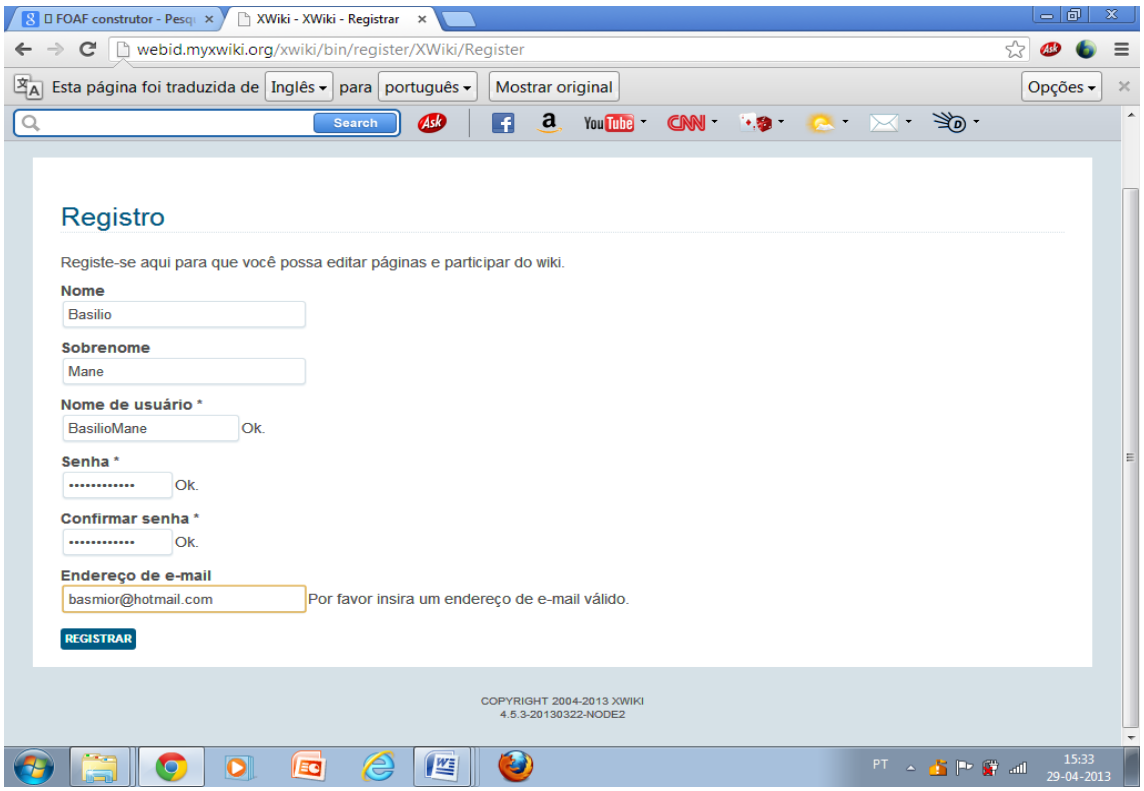

FIG. 3. Registro do utilizador na WebID

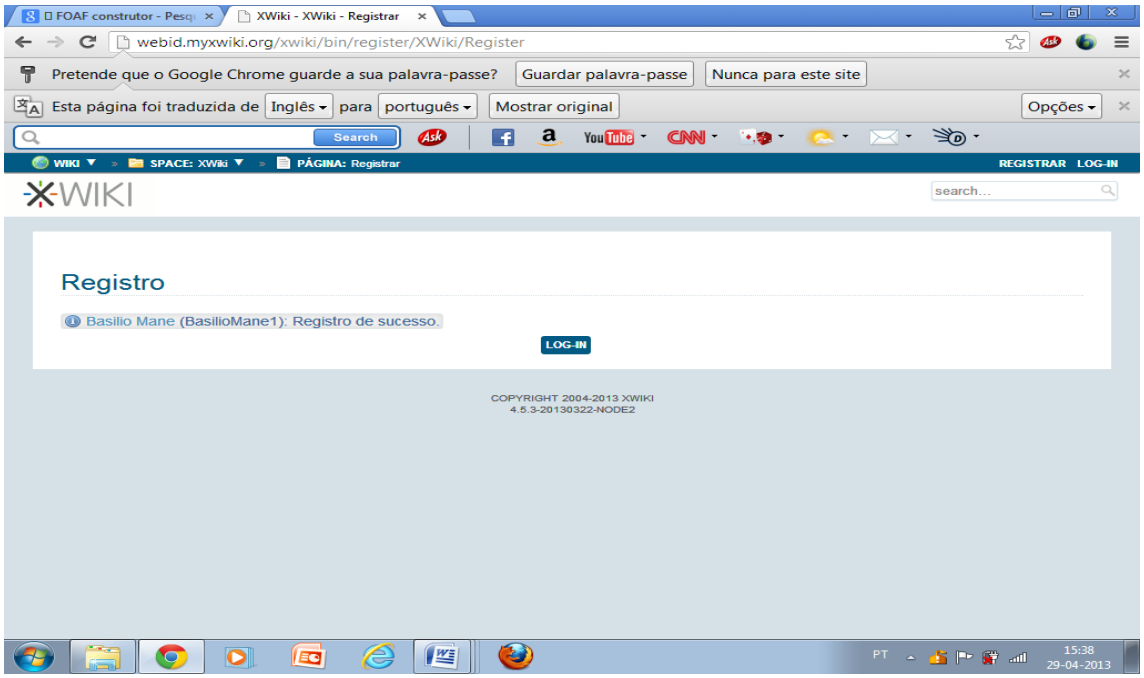

FIG. 4. Confirmação do registo de utilizador

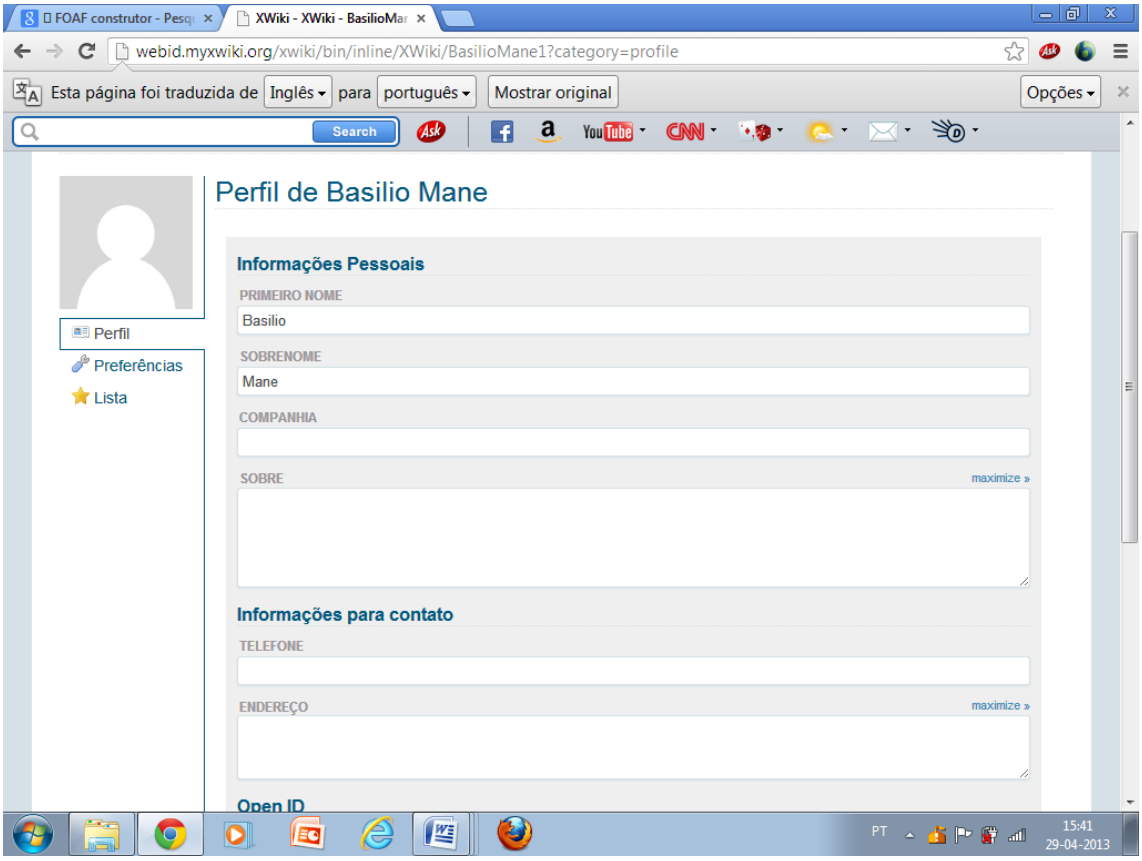

FIG. 5. Perfil de utilizador

Conclusão

No final deste trabalho, conclui-se que uma solução WebID é um substituto para o login tradicional na web. É um padrão aberto para a identidade digital. Com o WebID o utilizador não precisa mais de se lembrar de nomes de login ou senhas para todos os sites que usa. O utilizador pode publicar a sua identidade onde quiser e escolher que parte da sua informação pessoal deseja partilhar.

Referencias

http://www.w3.org/TR/2007/NOTE-grddl-primer-20070628

http://www.w3.org/TR/2004/REC-rdf-primer-20040210/

http://www.w3.org/TR/2004/REC-rdf-syntax-grammar-20040210

http://www.w3.org/TR/2012/REC-rdfa-core-20120607/

http://www.w3.org/TR/2008/NOTE-swbp-vocab-pub-20080828

http://www.w3.org/TR/turtle/

http://www.ietf.org/rfc/rfc2818.txt

http://www.w3.org/TeamSubmission/2008/SUBM-n3-20080114/

http://www.w3.org/TR/2004/REC-rdf-primer-20040210/

http://www.w3.org/TR/2004/REC-rdf-syntax-grammar-20040210

http://www.w3.org/TR/2011/WD-rdfa-core-20110331

http://www.w3.org/TeamSubmission/turtle/

http://www.w3.org/TR/2011/WD-xhtml-rdfa-20110331

http://www.w3.org/TR/2004/REC-rdf-concepts-20040210

http://www.w3.org/wiki/WebID

Anexos

Perguntas frequentes

Como é que um WebID se compara com o meu site de rede social?

Quando você receber uma conta no site de rede social favorita, como Facebook, MySpace , LinkedIn, gasta muito tempo dizendo ao site sobre si mesmo, quem são seus amigos, que fotos incluir e assim por diante. Esta informação é reutilizada para fornecer, dentro desse site, serviços como mostrar fotos de seus amigos. O problema é que cada site é um silo. Quando quiser usar informação que deu para um site em outro, tem que negociar para cada site para a aceder aos seus dados no outro.

Eu tenho uma homepage, que é o meu WebID?

Não, o URL da página Web identifica a localização de um documento que está associado ao utilizador, em certo sentido, é semelhante a sua carta de condução ou cartão de segurança social, esses dois artefactos podem identificá-lo indiretamente.

Uma vez que o utilizador não é um documento, o URL da página da Web não pode ser usado para construir um identificador que identifica de forma única o utilizador. Ele não pode ser o mecanismo de nomenclatura usada por outros utilizadores da Web.

O WebID é semelhante a um URL de uma homepage, mas especificamente identifica uma entidade "Você" do Tipo: Pessoa. Normalmente, a definição do Tipo: Pessoa, vem de um vocabulário ou dicionário de ontologia ou dados. Um tal vocabulário é o FOAF, que é a base deste esforço.

Quando o utilizador recebe um WebID, ele pode ser usado para referenciar "Você" com precisão. Ele também é o canal de toda a informação associada com "você", que inclui as coisas que o utilizador criou - Mensagens de blog, marcadores (bookmarks) partilhados, música, fotos, etc - e as relações que o utilizador tem com outras pessoas (sua rede social, por exemplo).

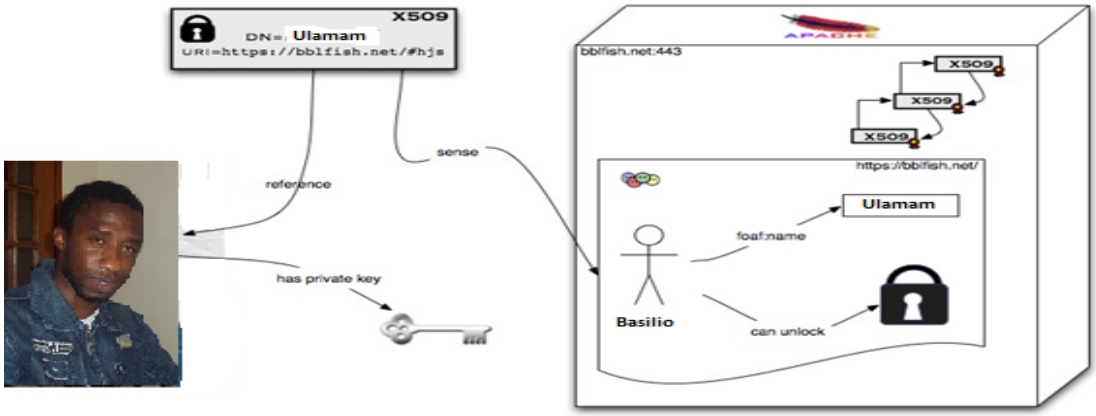

FIG. 6. Chave Pública WebId

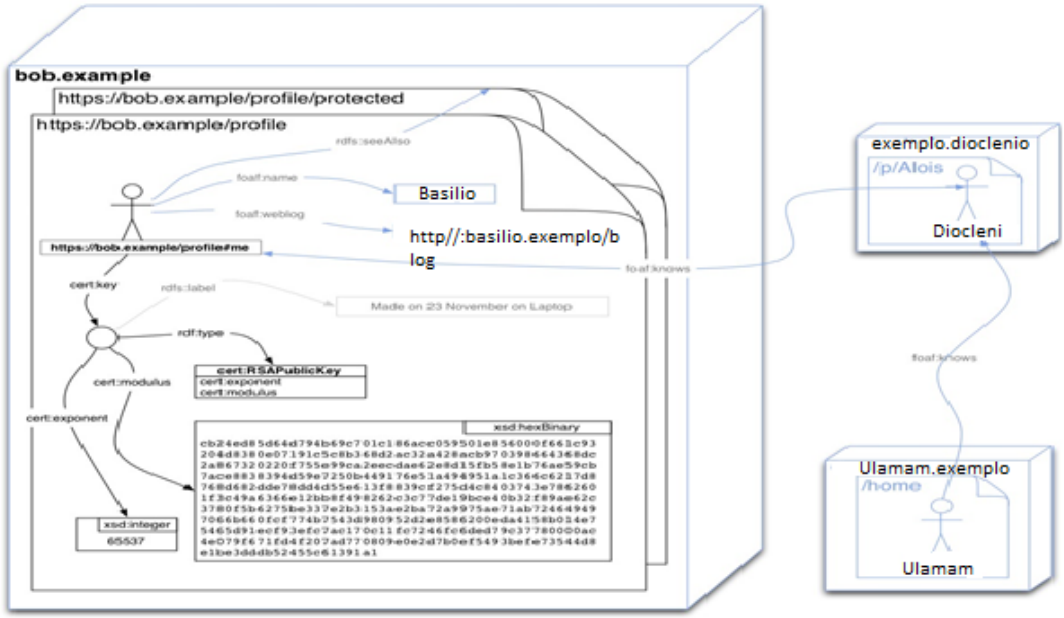

FIG. 7. Publicação do documento no perfil WebID

FIG. 8.9. Processo de instalação de software