Instituto Superior de Engenharia do Porto
Departamento de Engenharia de Electrotécnia
Mestrado em Engenharia Electrotécnica e de Computadores

Tese de mestrado

Plataforma de gestão e controlo de identidade digital e implementação novos modelos de governação e utilização das TIC

Autor: Paulo Filipe Gonçalves Calçada, aluno nº 1950433
Orientação: Prof. Dr. Miguel Leitão
Co-Orientação: Prof. Pedro Assis

Este relatório satisfaz, parcialmente, os requisitos que constam da Ficha de Disciplina de Tese/Dissertação, do 2º ano, do Mestrado em Engenharia Electrotécnica e de Computadores

Ano lectivo - 2011/2012

Novembro de 2012

Resumo

As estruturas orgânicas empresariais estão cada vez mais obrigadas a garantir elevados padrões de qualidade de serviços, possibilitando ao mesmo tempo a sustentabilidade das estruturas e ainda, o alinhamento dos investimentos efetuados com as estratégias de negócio. O seu desenvolvimento obriga a que na área das tecnologias de informação e comunicação exista a necessidade de repensar estratégias em vigor, procurando novos modelos, mais ágeis e mais capazes de se enquadrar nestas novas exigências.

Neste âmbito, é de esperar que as plataformas de identidade digital tenham um papel determinante no desenvolvimento destes novos modelos, pois são um instrumento único para se implementarem plataformas heterogéneas, interoperáveis, com elevados níveis de segurança e de garantia de controlo no acesso à informação.

O trabalho agora apresentado tem como objectivo investigar e desenvolver uma plataforma de identidade digital e uma plataforma de testes, que permitam ao Politécnico do Porto a aquisição de um infraestrutura de Tecnologias de Informação e Comunicação que se torne um instrumento fundamental para o desenvolvimento contínuo, de garantia de qualidade e de sustentabilidade de todos os serviços prestados à sua comunidade.

Palavras-Chave: Cloud Computing, TIC, Identidade Digital, Modelos de Governação

Abstract

In the current economic outlook, enterprises are being pushed to implement deep reorganization strategies, aiming at increasing the level and quality of services and, at the same time, reducing costs. ICT tools were always one of the development engines of medium and large enterprises. However, in the recent times, especially due to the increase of costs, CIOs have started searching for more agile and efficient ICT governance models. In this context, Identity Management Platforms are expected to play an important role in the development of heterogeneous, interoperable, secure and more efficient ICT platforms.

The main objective of this project is to investigate, develop and test an Identity Management Platform that will help Politécnico do Porto to cope with the challenges imposed by the new demands. At the same time it's also an objective of this project that the proposed a platform will be a unique tool for developing new, innovative, and sustainable services for Politécnico do Porto community.

Keywords: Cloud Computing, Identity Management, ICT, Governance Models

Índice

Lista de Figuras

Lista de Exemplos de Código

Acrónimos

ASN.1 - Abstract Syntax Notation – One
TIC - Tecnologias de Informação e Comunicação
ICT - Information and communication Technologies
CIO – Chief Information Officer
LDAP -Lightweight Directory Access Protocol
ITU-T - International Telecommunication Union - Telecommunication Standardization Sector
OID - Object identifier
ISO - International Standards Organization
ANA - Assigned Numbers Authority
TLS - Transport Layer Security
SAML - Security Assertion Markup Language
OASIS - Organization for the Advancement of Structured Information Standards
AAI – Authentication Authorization Infrastructure
REST - Representational State Transfer
NIST - National Institute of Standards and Technology
SSO - Single Sign-On
SASL - Simple Authentication and Security Layer
FCCN – Fundação de Computação Cientifica Nacional
IPP – Instituto Politécnico do Porto

1 – Apresentação

As estruturas orgânicas empresariais estão cada vez mais obrigadas a garantir elevados padrões de qualidade de serviços, possibilitando ao mesmo tempo a sustentabilidade das estruturas e ainda, o alinhamento dos investimentos efetuados com as estratégias de negócio. O seu desenvolvimento obriga a que na área das tecnologias de informação e comunicação exista a necessidade de repensar estratégias em vigor, procurando novos modelos, mais ágeis e mais capazes de se enquadrar nestas novas exigências.

Neste âmbito, é de esperar que as plataformas de identidade digital tenham um papel determinante no desenvolvimento destes novos modelos, pois são um instrumento único para se implementarem plataformas heterogéneas, interoperáveis, com elevados níveis de segurança e de garantia de controlo no acesso à informação.

O trabalho agora apresentado teve como principal objectivo desenvolver uma plataforma de identidade digital capaz de impulsionar a adopção dos novos modelos de governação das Tecnologias de Informação e Comunicação (TIC). Este tema é considerado de grande relevância, em especial no que refere aos possíveis ganhos de eficiência e eficácia, que os novos modelos de governação TIC podem trazer para organizações, de média e grande dimensão. Este trabalho utilizou como caso de estudo a plataforma TIC do Instituto Politécnico do Porto (IPP). Para além da dimensão, esta plataforma permitiu aceder a um ambiente heterogéneo em termos de organização e, em termos de perfis de utilização, que se demonstrou fundamental para atingir os objectivos a que nos propusemos.

1.2 Contexto e plano de trabalho

A plataforma TIC do Politécnico do Porto sofreu uma profunda reorganização com a execução do projecto IPPwnet, com início no ano de 2003, este projecto tinha como objectivo principal modernizar as plataformas TIC existentes em todas as unidades IPP, e em especial, o conjunto de serviços que eram disponibilizados pelos seus serviços centrais. Como resultado imediato deste trabalho, foi possível identificar sinergias entre as várias unidades, que através da partilha de recursos, contribuiriam para a maximização do retorno dos investimentos efectuados e para o aumento da qualidade dos serviços.

A necessidade de melhoramento contínuo dos serviços oferecidos à sua comunidade, assim como a necessidade de acompanhar as evoluções tecnológicas e de gestão, garantindo sempre um correta utilização dos recursos disponíveis, estão na base do projecto promovido pelo Politécnico do Porto para o desenvolvimento da "*Plataforma de gestão e controlo de identidade digital e implementação de novos modelos de governação e utilização das TIC",* que serve de base à tese de mestrado agora apresentada. Tendo como principal objectivo adequar a plataforma de tecnologias de informação e comunicação (TIC) que o Politécnico do Porto tinha vindo a desenvolver até então, às práticas de referência internacional, este projecto apresenta ainda, como objectivo complementar, a criação de uma estratégia de sustentabilidade futura.

Com a apresentação do projecto de criação da "*Plataforma de gestão e controlo de identidade digital e implementação de novos modelos de governo e de utilização do TIC",* o Politécnico do Porto pretendeu dar continuidade aos resultados do projecto IPPwNet, nomeadamente na componente de partilha de recursos e modelos de governação. Para

isso foi definido um novo plano de acção, acrescentando os seguintes objectivos:

- Criação de serviços mais interactivos e com experiência de utilização mais rica;
- Garantia de consolidação dos investimentos feitos até então, nomeadamente na componente de infra-estrutura, segurança, controlo de acessos e monitorização;
- Criação de plataforma tecnológica de referência nacional;
- Definição de modelo de sustentabilidade e melhoria continua.

Com a intenção de concretizar os objectivos definidos, o trabalho agora apresentado definiu uma estratégia assente em dois grandes vectores, descritos em seguida:

- Acompanhamento das tendências tecnológicas potenciando a sustentabilidade e retorno do investimento a curto e médio prazo – processo em contínuo desenvolvimento com medidas de curto prazo inseridas numa visão e estratégia holística de longo prazo;
- Harmonização, normalização e modularização tecnológica – modularidade no desenvolvimento, em articulação com a estratégia definida no ponto anterior (visão no médio/longo prazo).

A conjunção entre os objectivos definidos e a estratégia escolhida permitiu definir um plano de trabalhos assente nas seguintes acções:

- Desenvolvimento de plataforma de identidade digital para toda a comunidade;
- Implementação de uma plataforma de teste.

Como resultado das acções propostas espera-se garantir que o Politécnico do Porto passe a possuir uma plataforma TIC que se torna num instrumento fundamental para o desenvolvimento contínuo, de garantia de qualidade, e de sustentabilidade, de todos os serviços prestados à sua comunidade.

2 – Enquadramento

2.1 – Da Internet à Web 2.0

No seguimento da evolução quase vertiginosa a que se assistiu durante a década de 90 do século passado, e do consequente *crash d*o início deste novo milénio, a Internet entrou num processo de reorganização tecnológica e de procura de modelos de negócio que suportassem as necessidades de consolidação a que foi obrigada. Este processo de reajuste permitiu também que, de forma não orquestrada, fosse efetuada uma reaproximação entre as tecnologias e as necessidades dos utilizadores. A multiplicidade de serviços que até à data existiam: *Cha*t (IRC); Páginas de conteúdos (HTTP); Partilha de ficheiros (FTP); Noticias; Fóruns, muitos deles com fortes componentes de interação social, passaram a ser disponibilizados de forma mais estruturada, concentrando-se quase maioritariamente numa única estrutura tecnológica. O HTTP e as tecnologias relacionadas, que suportam a disponibilização de páginas de conteúdos, a que vulgarmente se chama de Web, passou a ser dominante. As evoluções tecnológicas que entretanto surgiram permitiram que o conjunto de serviços anteriormente disponibilizados por estruturas independentes, passasse a ser acessível por uma única plataforma tecnológica - a janela do nosso navegador Web (*browser*).

Simultaneamente, e sem uma decisão prévia ou uma intencionalidade declarada, este processo de reorganização contribuiu significativamente para o reforço das características de interacção social que a Internet possuía. No sentido de dar resposta à crescente procura de novos utilizadores, cada vez mais interessados neste novo tipo de oferta que a Internet proporciona, mais exigentes, e ao mesmo tempo mais dependentes dos serviços disponibilizados, surge um conjunto de desenvolvimentos tecnológicos e de modelos de negócio que nos “prendem” ao *browser* e, aos quais, é vulgarmente dado o nome de WEB 2.0.

A WEB 2.0 apresenta uma nova filosofia de utilização mais focada na interacção social, apresentando também um novo tipo de utilizadores, habituados a crescer com a Internet. Se a Internet foi no passado uma enorme biblioteca, passou com esta transformação a ser uma enorme sala de convívio. A criação de redes de contacto e redes sociais é hoje um dos polos de atracão e um dos motores da Internet. Serviços como o Hi5, Linkedin.com, YouTube, Facebook. e MySpace, são exemplos de como a Web 2.0 consegue atrair e, principalmente, como consegue potenciar e dinamizar a troca de informação e conhecimento.

Para que esta evolução fosse possível foi necessário que um conjunto de factores estivessem alinhados. Para além da mudança do perfil de utilização, foi ainda determinante o aparecimento de um grande conjunto de evoluções tecnológicas assim como de novos modelos de negócio. Na figura 1 são apresentados de forma resumida os vários factores que contribuíram para esta transformação, assim como alguns dos grandes benefícios que a Web 2.0 proporciona.

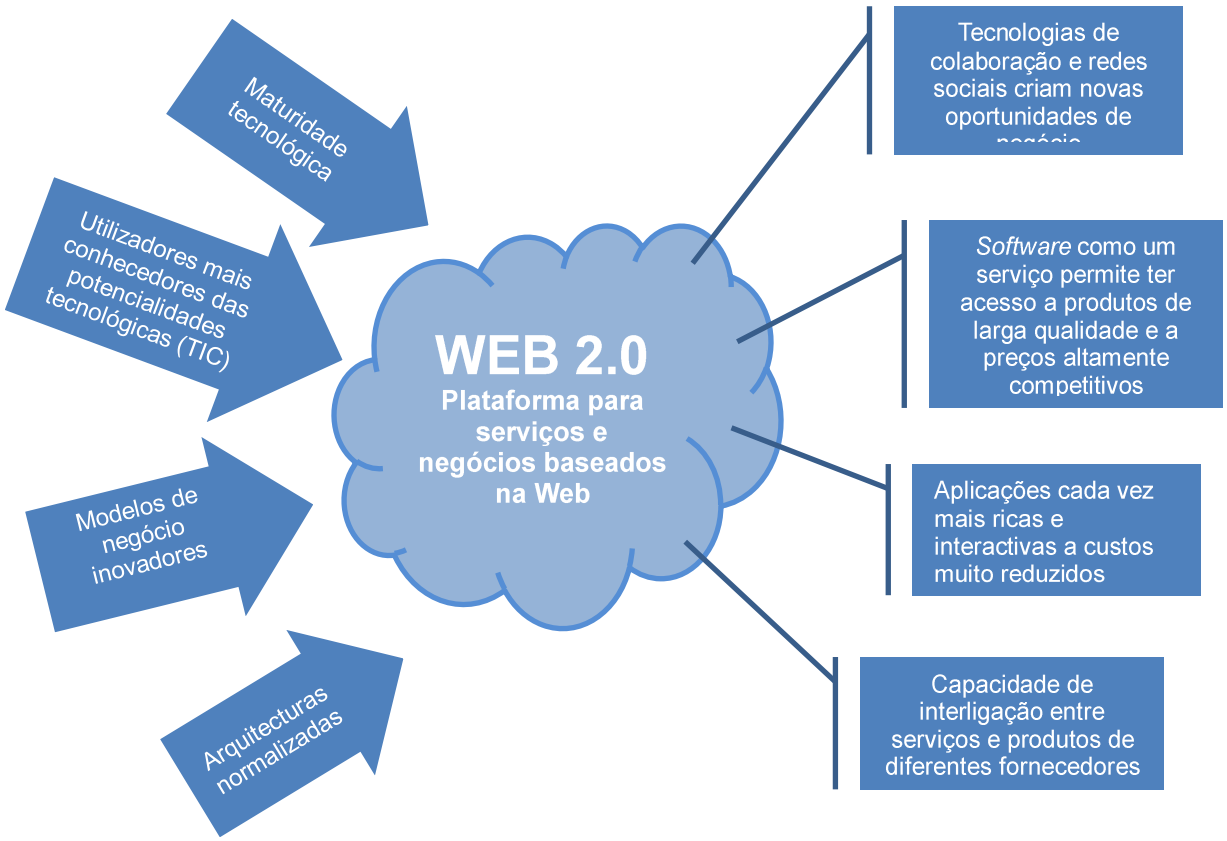


Figura 1 - Web 2.0

Estudos recentes da consultora McKinsey, demonstram que o impacto da WEB 2.0 nas organizações, nomeadamente através da utilização de plataformas colaborativas, que interligam as equipas internas a parceiros externos, tem sido muito elevado. Em concreto, e segundo os dados dos estudos, as organizações passam a beneficiar directamente em algumas destas áreas:

- Obter informação sobre produtos e soluções mais rapidamente;
- Aumentar a eficácia das estratégias de marketing;
- Reduzir custos de comunicação.

Segundo estes estudos, cerca de 40% das organizações usam actualmente redes sociais como ferramentas de interação, e cerca de 38% recorrem a *blogs*. É importante constatar ainda que cerca de 50% das organizações que possuem redes sociais, referem que pelo menos 51% dos seus funcionários são utilizadores regulares destas redes.
Em termos de impacto nos negócios, é muito importante referir ainda que 79% das organizações referem que conseguem ganhos médios directos na ordem dos 5%.

2.2 – Novos Modelos de Governação TIC em Ambientes Empresariais

A importância e relevo da Internet para organizações em geral, começou a ser reconhecida ainda antes do aparecimento do fenómeno "Web 2.0". Isto aconteceu graças à criação de portais institucionais, normalmente focados na promoção da imagem corporativa, ou em alguns casos, através da apresentação de estratégias inovadores na área e *e-commerce,* dinamização da relação com os clientes e parceiros, entre outros exemplos. É inevitável relacionar o impacto da Web 2.0 no desenvolvimento das estratégias de utilização das TIC pelas organizações em geral.

Para além das evoluções tecnológicas que entretanto foram sendo introduzidas, e que serviram de catalisadores de desenvolvimento das TIC, o aparecimento do novo tipo de utilizadores – cada vez mais dependentes dos serviços oferecidos pela Web 2.0, obriga a uma reorganização mais profunda das estratégias de disponibilização de infraestruturas TIC empresariais. Ao mesmo tempo que os utilizadores comuns passam a exigir que as tecnologias proporcionem formas mais interactivas e apelativas de utilização, as organizações começam também a identificar novas oportunidades para reposicionar as TIC como agentes de dinamização dos seus modelos de negócio.

Em complemento ao movimento de procura de novas estratégias de utilização, as organizações começam também a reconhecer que as TIC possuem, na maioria dos casos, um peso demasiado elevado na sua estrutura de custos. Em seguida são apresentados alguns dos factores considerados pelos responsáveis empresariais nesta análise:

- Custos elevados de aquisição e manutenção, normalmente devido aos modelos de negócio apresentados pelos fornecedores TIC;
- Elevada complexidade tecnológica, que obriga à contratação de recursos humanos altamente qualificados,
- Reduzida capacidade das soluções e modelos TIC para acompanhar os modelos de desenvolvimento das organizações.

Como foi apresentado anteriormente, e sendo ainda de salientar o facto de que cada vez mais as organizações são obrigadas a procurar modelos de desenvolvimento mais ágeis e capazes de acompanhar as evoluções dos mercados, o desenvolvimento de novos modelos de governação TIC então a ser considerados uma prioridade pela maioria das organizações.

De acordo com estas novas exigências, as TIC necessitam de dar resposta a um conjunto de desafios tecnológicos e de modelo de negócio, nomeadamente: a) elasticidade, ou seja a capacidade de alocar recursos à medida que estes são necessários; b) elevada tolerância a falhas; c) capacidade de gestão e aprovisionamento de recursos; d) elevada segurança; e) elevado desempenho; f) simplicidade de utilização; g) redução do investimento inicial, permitindo realocar recursos financeiros.

Com base no desenvolvimento dos conceitos apresentados pela Web 2.0, e no sentido de ser criado um modelo mais abrangente, onde as tecnologias de informação e comunicação são disponibilizadas de forma descentralizada, com altos níveis de serviços, segurança e agilidade na sua configuração, surge o conceito de Cloud Computing. Para o sucesso actual do modelo de Cloud Computing contribuíram ainda todos os modelos que surgiram nos últimos anos, e que permitiram avanços no desenvolvimento e na gestão

das plataformas TIC, de que são exemplos os fornecedores de aplicações ASP (Aplication Service Provider) e a arquitetura SOA (Service Oriented Architectures). No entanto o desenvolvimento do paradigma Cloud Computing veio permitir reunir no mesmo modelo, as condições necessárias e suficientes para potenciar o desejado realinhamento das TIC ao ambiente empresarial, criando verdadeiros agentes catalisadores de inovação e desenvolvimento.

O Cloud Computing procura resolver um conjunto de problemas e desafios actuais: a agilidade na gestão, manutenção e aprovisionamento de recursos; a elasticidade em os disponibilizar a pedido; a tolerância a falhas, segurança e elevada disponibilidade; a interoperabilidade entre sistemas; o maior controlo de custos no acesso a serviços de tecnologia e, acima de tudo, simplicidade na sua concretização. A mudança ao nível do modelo de negócio, tendo por base o conceito "pay-per-use", permite a redução do custo inicial do serviço disponibilizado.

Como modelo disruptivo, o Cloud Computing aborda, de forma simplificada e flexível, as TIC numa perspetiva de serviço, e organizado em três grandes áreas de ação: Sofware-as-a-Service (SaaS), Platform-as-a-Service (PaaS) e Infraestruture-as-a-Service (IaaS). Estas áreas refletem diferentes níveis de serviço que o cliente pode usufruir. Na camada SaaS o utilizador faz uso das aplicações disponibilizadas pela nuvem. Na camada PaaS, o utilizador usa a nuvem para disponibilizar, ele próprio, as suas aplicações. Por último, na camada IaaS, o utilizador usa os recursos da nuvem para desenvolver plataformas de suporte às aplicações.

Na figura 3 é apresentado um diagrama simplificado das várias áreas que constituem o modelo de Cloud Computing.

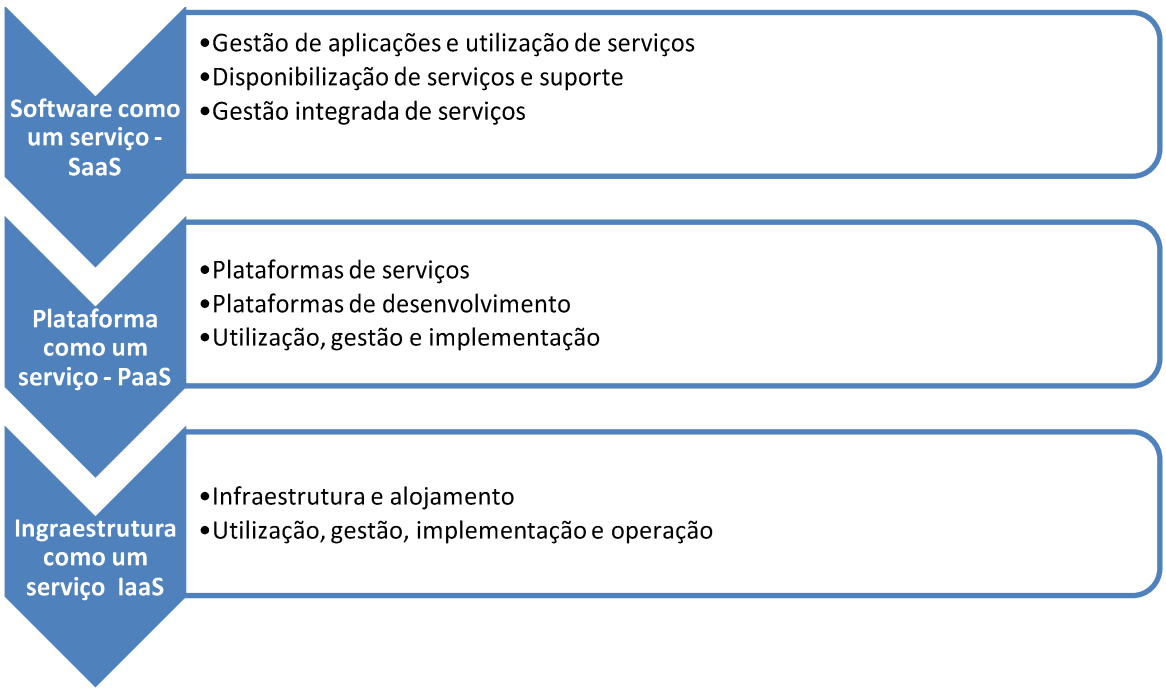


Figura 2- Cloud Computing – Cadeia de Valor

Apesar de ainda se encontrar numa fase de desenvolvimento inicial, e de haver um grande conjunto de questões tecnológicas e de legislação para serem resolvidas [3], nomeadamente na área da segurança e protecção de dados, localização da informação, entre outros, os produtos e soluções baseados em Cloud Computing têm sido cada vez mais procuradas pelas organizações. De salientar ainda que segundo dados da Comissão Europeia, é de esperar que a aposta neste modelo possa ter um impacto na economia Europeia até 2020 na ordem dos 160 mil milhões de Euros, e que permita ainda criar cerca de 2.5 milhões de postos de trabalho [4][5].

Para além da aposta que a Comissão Europeia é de salientar ainda o grande número de estratégias de desenvolvimento do modelo de Cloud Computing, que vários outros países também se encontram a promover [6][7]. Esperando-se assim que venham a contribuir decisivamente para a completa mudança do paradigma de utilização e disponibilização das TIC em termos mundiais.

2.2.1 – Cloud Computing como Modelo de Referência

Apesar de nem sempre ter sido consensual, actualmente é recorrente utilizar a definição do Cloud Computing apresentada pelo NIST [8]. Segundo esta definição o *Cloud Computing*, é um modelo de computação constituído por cinco características essenciais: utilização *self-service*, acesso através da rede, disponibilidade de recursos, rápida elasticidade e mensuração do serviço.

Em seguida são apresentados de forma detalhada as características principais do Cloud Computing segundo o modelo definido pelo NIST.

Utilização Self-Service
Um consumidor pode, unilateralmente, dispor de recursos de computação, como o tempo de processamento, armazenamento e servidores de rede, automaticamente, conforme as suas necessidades e sem que seja necessária a interação humana.

Para serem eficazes e aceitáveis para o consumidor, as interfaces gráficas, pelas quais os consumidores interagem com o produtor, devem ser de fácil utilização e proporcionar meios eficazes para gerirem a oferta de serviços. A facilidade de utilização e eliminação de interação humana proporciona ganhos de eficiência e redução de custos, tanto para o utilizador, como para os produtores de serviços.

Acesso através da rede
Os recursos estão disponíveis através da rede e são acedidos por meio de mecanismos normalizados, que promovem o uso por plataformas heterogéneas, como por exemplo: telemóveis, computadores portáteis, e PDAs.

Para que este modelo de computação seja uma alternativa efectiva aos *data-centers in-house*, deverão existir ligações de banda larga que liguem os consumidores aos serviços *cloud*.

Disponibilidade de recursos
Os recursos estão organizados de forma a servirem múltiplos consumidores, usando um modelo *multi-tenant*, recorrendo a diferentes recursos físicos e virtuais e de acordo com a procura do cliente.

O utilizador não tem controlo ou conhecimento da localização exata onde estão os recursos, mas poderá existir a possibilidade de definir, em alto nível, a sua localização. Este modelo de computação, deverá possuir um vasto leque de recursos de forma a poder responder às necessidades dos clientes, atingir economias de escala e respeitar a qualidade de serviço contratado. As aplicações precisam de recursos para a sua execução e esses deverão ser alocados eficientemente para uma ótima performance, mesmo que estejam localizados em áreas geográficas dispersas.

Rápida elasticidade
Os recursos deverão ser fornecidos de uma forma rápida e elástica, e em algumas situações de forma automática, de forma a assegurar a escalabilidade do sistema. Para o consumidor, os recursos deverão parecer ilimitados, podendo ser adquiridos em qualquer número e altura, cujo custo resultará do tempo de utilização e quantidade de recursos consumida.

Esta característica diz respeito à habilidade de rapidamente aumentar ou diminuir os recursos alocados, de forma a cumprir com os requisitos de *self-service*.

Mensuração do serviço
Estes sistemas de computação controlam e otimizam a utilização de recursos, automaticamente, e de acordo com os níveis apropriados para o tipo de serviço a título de exemplo, armazenamento, processamento, largura de banda e número de contas activas. A utilização de recursos pode ser monitorizada, controlada e comunicada, tornando o serviço transparente, tanto para o consumidor, como para o produtor.

Em virtude das características deste modelo de computação, o número de recursos consumido, poderá ser monitorizado e definido de forma dinâmica. Dessa forma, serão depois faturados os consumos relativos aos recursos alocados para uma determinada sessão.

2.2.2 – Cloud Computing e os Modelos de Distribuição

Por forma a responder aos níveis de serviço exigido pelos diferentes perfis de empresa, o Cloud Computing apresenta quatro níveis de distribuição, apresentados de forma detalhada em seguida.

Cloud Publica - Public Cloud
A infra-estrutura de *Cloud Computing* está disponível ao público em geral, ou a um grande grupo industrial, sendo propriedade de uma organização que comercializa serviços de *Cloud Computing.* Este tipo de modelo de distribuição é o mais comum, os serviços são disponibilizados aos clientes através de um fornecedor, sendo que os recursos disponibilizados são partilhados com outros clientes. A segurança e a governação dos dados são as maiores preocupações desta abordagem.

Cloud Privada - Private Cloud
A infra-estrutura de *Cloud Computing é* operada unicamente por uma organização, podendo existir dentro ou fora das instalações, sendo gerida pela própria organização ou por uma outra entidade. Muitas destas infra-estruturas são operadas por grandes empresas, ou departamentos governamentais, que preferem manter os seus dados num ambiente mais controlado e seguro.

Cloud Comunitária - Community Cloud

A infra-estrutura da *Cloud Computing é* partilhada por diversas organizações, suportando uma comunidade com idênticas preocupações (ex: missão, requisitos de segurança, politicas, etc.), podendo existir dentro ou fora das instalações, sendo gerida pelas organizações que a compõem, ou por uma entidade.

Cloud Hibrida - Hybrid Cloud
A infra-estrutura da *Cloud Computing é* uma composição de duas ou mais nuvens (infra-estruturas de *Cloud Computing* privadas, comunitárias, ou públicas) que permanecem entidades únicas, e que estando ligadas, através de tecnologia *standard* ou proprietária, permitem a portabilidade de dados e aplicações. Desta forma, uma organização poderá manter os seus dados e aplicações críticas, dentro das suas instalações, colocando as menos críticas numa infraestrutura de *Cloud Computing* publica.

2.2.3 – Cloud Computing e os Modelos de Serviço

Os recursos disponibilizados pelo Cloud Computing, que podem incluir *hardware*, ambientes de programação, ou aplicações, entre outros, estão organizados em três modelos de serviço: *Infrastructure as a Service (IaaS)*, *Platform as a Service (PaaS)*, e *Software as a Service (SaaS)*.

Através dos modelos de serviço apresentados, as diferentes organizações poderão desempenhar papéis diferentes na construção e utilização de sistemas *Cloud Computing*. Esses papéis variam entre *Technology Enablers* (disponibilizam as tecnologias que tornam possível este modelo de computação), *Cloud Providers* (distribuem as suas infra-estruturas e plataformas aos clientes), *Cloud Customers* (recorrem aos fornecedores para melhorar as suas aplicações Web) e *Cloud Users* (utilizam as aplicações Web, sem possivelmente saber que estão alojados na *cloud*).

Em seguida apresenta-se de forma detalhada os diferentes modelos de serviço.

Infrastructure as a Service (IaaS)
É colocado á disposição do consumidor tempo de processamento, armazenamento, redes e outros recursos de computação fundamentais, podendo o consumidor alojar e executar qualquer software, incluindo sistemas operativos e aplicações.
O consumidor não gere ou controla a infra-estrutura base, mas tem controlo sobre o sistema operativo, armazenamento, alojamento de aplicações, podendo ter a possibilidade de controlar um leque limitado de componentes de rede (ex: *firewall*).

Platform as a Service (PaaS)
É possibilitado ao consumidor o alojamento, na infra-estrutura, de aplicações criadas ou adquiridas pelo consumidor, desde que desenvolvidas em linguagens de programação/ferramentas suportadas pela infra-estrutura.

O consumidor não gere ou controla a infra-estrutura base, incluindo rede, servidores, sistemas operativos ou armazenamento, mas tem controlo sobre as aplicações alojadas, e possivelmente pode controlar as configurações de alojamento das aplicações.

Software as a Service (SaaS)
O consumidor não gere ou controla a infra-estrutura base, incluindo a rede, servidores, sistemas operativos, armazenamento, ou até mesmo recursos das próprias aplicações, excluindo-se a configuração de alguns parâmetros, específicos do utilizador.

É permitido ao consumidor a utilização de aplicações disponibilizadas pelo produtor. As aplicações podem ser acedidas através de vários dispositivos clientes, mediante um interface gráfico como um *browser* ou similar.

Na figura seguinte é apresentado um resumo dos modelos de serviço de Cloud Computing, com indicação de algumas das empresas fornecedoras de referência. Estes modelos de serviço são na sua maioria disponibilizados através do modelo de distribuição de Cloud Publica, podendo no entanto ser também usados em modelos híbridos.

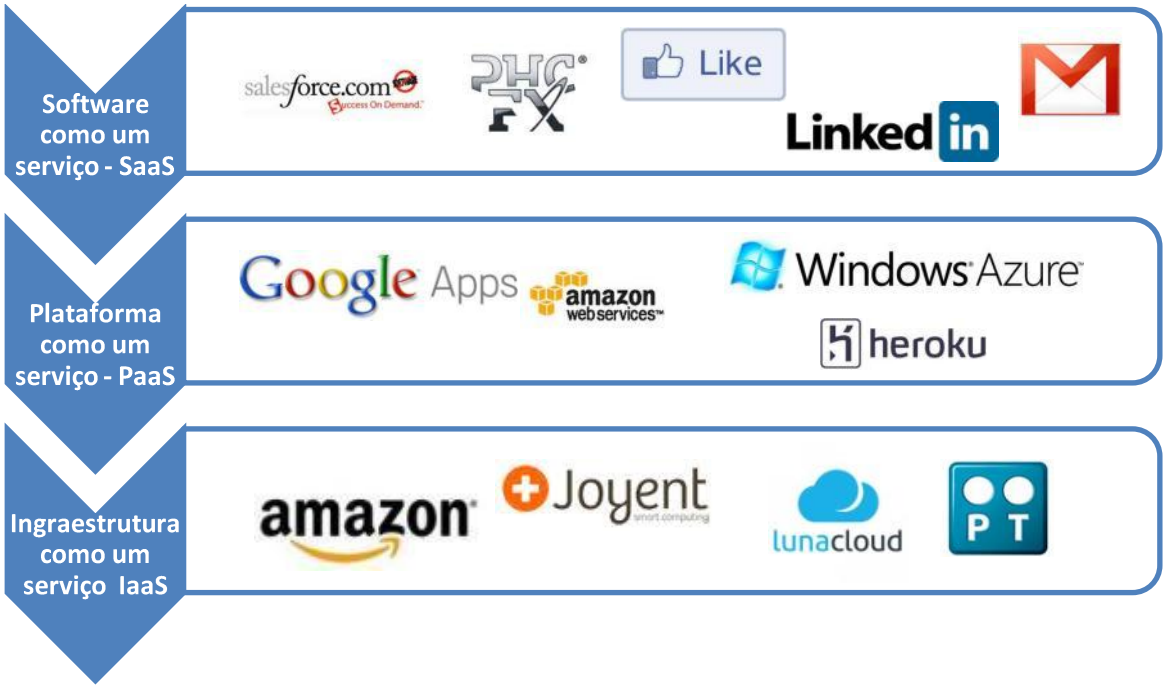


Figura 3 - Fornecedores de Cloud Computing de referência

2.3 – A Identidade Digital como Fator de Desenvolvimento da Internet

Nos primórdios da Internet a capacidade de aceder a um recurso através de um simples clique num *hyperlink* era algo de extraordinário. No entanto, e devido ao desenvolvimento tecnológico, e ao consequente alargamento do seu âmbito de utilização, rapidamente passou a existir na Internet a possibilidade de um individuo utilizar os sistemas de forma mais rica e interactiva.

Esta transformação da Internet, que passou de um sistema de publicação de conteúdos estático, para uma plataforma de interacção e de entrega personalizada de serviços – comércio electrónico, governo electrónico, redes sociais, etc. Ficou definitivamente ligada à possibilidade de indivíduos estabelecerem interacções personalizadas, e de passarem a ser reconhecidos pelos sistemas remotos – a sua identidade passou a ser um fator de decisão na capacidade de interacção. O desenvolvimento da identidade digital foi um avanço extraordinário, que possibilitou uma década de inovação, e que transformou a Internet em algo indispensável para o desenvolvimento das nossas sociedades.

2.3.1 – A Importância da Identidade em Ambientes Heterogéneos

Segundo o dicionário Português, identidade define-se como: "*Circunstância de um indivíduo ser aquele que diz ser ou aquele que outrem presume que ele seja".* Na nossa sociedade, esta circunstância é validada geralmente com base em dados suportados por um documento, seja ele o cartão do cidadão, a carta de condução, ou um simples número de registo. Do ponto de vista digital, a identidade está relacionada com a gestão, protecção e controlo do acesso à informação num ambiente digital. De forma simplificada, poder-se-á dizer que representará a versão digital de um individuo (sujeito). Segundo alguns autores, nomeadamente Phil Windley [9], a identidade digital contem informação sobre o sujeito, pessoa ou coisa, contendo adicionalmente informação de contexto que o relaciona com diferentes entidades.

Como referido anteriormente, no "mundo real", a identidade de um sujeito é validade através da verificação, normalmente visual, de um documento, que em determinados casos de acesso mais reservado, deve também ser acompanhado de uma credencial ou declaração ("claim"). Nos ambientes digitais este processo de verificação é mais complexo, pois, por exemplo, o sujeito que apresenta a declaração pode nem sempre ser uma pessoa. Em ambientes digitais existe uma enorme diversidade de agentes (sujeitos) que podem ter um identificador, uma identidade.

No ambiente digital, assim como no ambiente "real", para que uma identidade seja reconhecida e validada é importante que se tenha como referência a necessidade de existência das seguintes componentes: o identificador; e o autenticador. O identificador é um nome único, usado para referenciar o sujeito, sem haver a necessidade de referir alguma das suas partes, ou propriedades em específico. A segunda componente, o "autenticador", determina a legitimidade que o sujeito tem em reclamar (declarar) a sua identidade.

Como exemplo, no acesso a um computador, ou sistema, é normalmente usado um mecanismo simples baseado em um "Nome de utilizador", o identificador, e uma "Palavra-chave", o "autenticador".

Na figura seguinte é feito uma apresentação simplificada dos vários elementos que constituem um sistema de identidade digital.

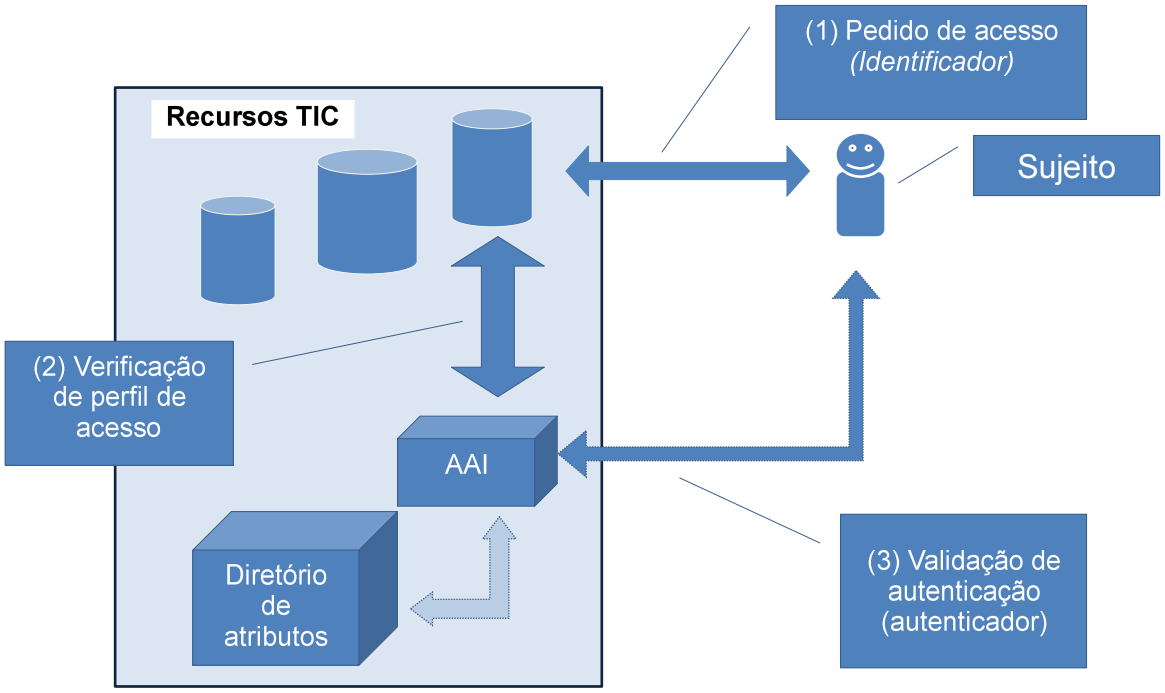


Figura 4 – Utilização de plataformas de Identidade Digital

2.3.2 - A Identidade Digital e os Modelos de Governação TIC

Como foi apresentado na secção anterior, os novos modelos de governação TIC, em especial devido à necessidade de possuírem uma elevada flexibilidade, têm por base uma estrutura heterógena de serviços e fornecedores. Se até então era possível controlar o ambiente de disponibilização de serviços TIC de forma segura, nomeadamente devido ao fato de a maioria dos recursos se encontrarem instalados em estruturas da própria organização, com o aumento da importância dos novos modelos de governação TIC, nomeadamente com o surgimento do Cloud Computing, passa a ser obrigatório desenvolver novas estratégias de controlo do acesso a toda a plataforma TIC.

As plataformas de identidade digital, ou de controlo de acesso dos utilizadores aos recursos TIC, foram, desde o início da utilização das tecnologias de informação, uma das principais áreas de trabalho das equipas de gestão e desenvolvimento. Se inicialmente o controlo dos utilizadores era feito através de mecanismos simples de identificação, normalmente recorrendo a um par identificador-palavra chave, com o decorrer dos tempos e, com o aumento da complexidade das estruturas TIC, foi necessário desenvolver mecanismos mais complexos. Com a introdução das Infraestruturas de Autenticação e Autorização (AAI – *Authentication Authorization Infrastructures*) as organizações passam a possuir mecanismos que, para além de garantirem a correta identificação dos seus utilizadores, permitem também que o controlo do acesso aos recursos passe a ser

efetuado em função dos atributos dos utilizadores e do contexto de utilização.

Na figura seguinte é apresentado um esquema com a relação entre os diferentes componentes de uma estrutura de identidade digital.

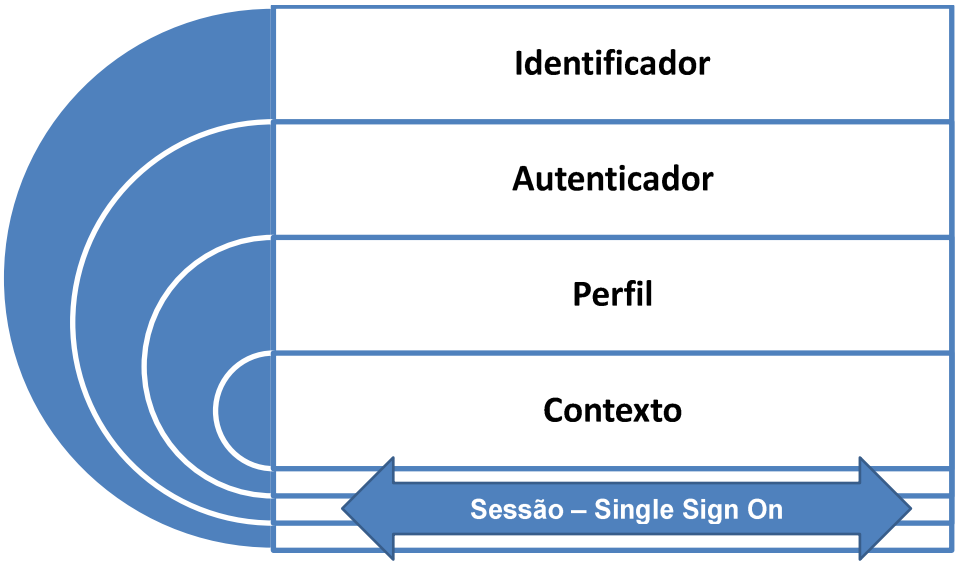


Figura 5 – Componentes de uma Infraestruturas de Autenticação e Autorização

Mais do que simples plataformas para controlar o acesso aos serviços, através de processos de autenticação, as plataformas de AAI são ferramentas fundamentais para permitir contextualizar o processo de acesso aos recursos – implementar mecanismos de autorização. Pelo facto de estarem normalmente integradas com repositórios de informação dos utilizadores e das organizações, permitem fornecer um controlo efectivo e completo aos recursos. Adicionalmente as plataformas de AAI possuem ainda mecanismos de gestão de sessões. Estes mecanismos são fundamentais para que um utilizador possa utilizar os recursos em ambientes heterogéneos, com os encontrados actualmente nas organizações, onde os serviços são disponibilizados por vários fornecedores, que normalmente não possuem qualquer tipo de integração adicional, que não a disponibilizada pelas plataformas de AAI. A estes mecanismos de gestão de sessões é dado o nome de sistemas de Single-Sign-On (SSO).

2.3.3 – Modelos de Implementação das Plataformas AAI

Historicamente as plataformas de TIC organizam as “identidades” dos utilizadores em silos fechados dentro de aplicações ou de ecossistemas muito restritos. Pelo facto de normalmente estes silos não permitirem o fluxo de informação dos utilizadores entre aplicações, ou mesmo para fora dos referidos ecossistemas, comportam-se como verdadeiras barreiras ao desenvolvimento das plataformas TIC, e consequentemente das próprias organizações. Com o decorrer dos tempos, e com a exigência de uma maior interoperabilidade entre sistemas, a capacidade de permitir o aumento deste tipo de transacções passou a ser um requisito obrigatório para todas as organizações.

Em seguida é efectuada uma apresentação dos vários sistemas que actualmente podem ser considerados, sendo também feita uma descrição de algumas das principais diferenças entre ambos.

Sistema de Identidade Digital em Silo

Um sistema de identidade digital em silo é o modelo mais simples e que é desenvolvido para operar de forma independente, sem qualquer tipo de ligação formal a sistemas externos. No entanto é importante referir, que de forma informal, e quase naturalmente, os sistemas de silo têm ligações a sistemas de identidade externa. Por exemplo, quando recorrem à data de nascimento de uma pessoa, ou ao numero de identificação do cartão de identificação. Um das grandes vantagens do sistema de silo está no facto de em caso de problema ou anomalia, por exemplo por uso abusivo das credenciais, o impacto ser reduzido, pois fica unicamente limitado ao sistema em questão. No entanto, o facto de este sistema ser fechado, de não permitir a reutilização das credenciais, pelo menos de uma forma uniformizada e automática, representa um grande inconveniente. Á medida que o número de sistemas a que um utilizador tem acesso aumenta, será também mais complexo gerir as credenciais de forma segura. Adicionalmente, este tipo de sistemas representa também uma redução na eficiência dos recursos à medida que as organizações vão crescendo, pois haverá sempre uma grande redundância de equipamentos e sistemas.

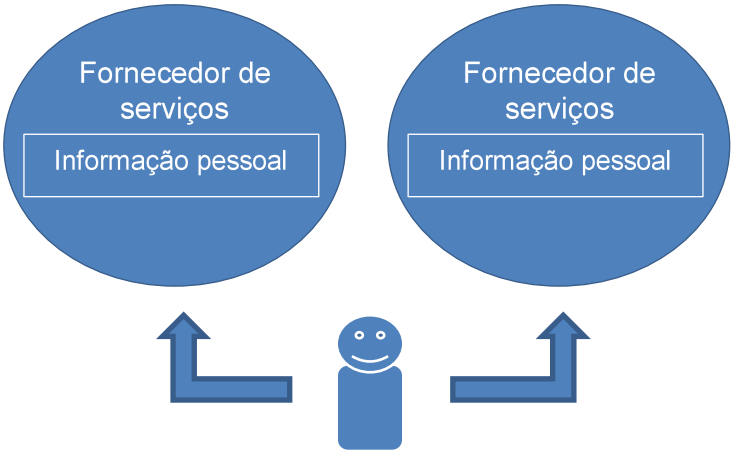


Figura 6 – Sistema de Identidade Digital em Silo

Sistema Centralizado de Identidade Digital
No sentido de resolver alguns dos problemas apresentados pelos sistemas em silo, nomeadamente a duplicação de recursos, surge o sistema centralizado de identidade digital.
Neste sistema as credenciais de um utilizador, e todos os dados de controlo de acesso, são guardados num sistema central. Este sistema central, que normalmente possui o formato de directório de informação, é então utilizado por vários recursos. Os diretórios de informação foram sendo desenvolvidos de forma muito activa durante os últimos anos, o que lhes permitiu passarem a possuir capacidade de alojamento de informação muito distinta e específica.

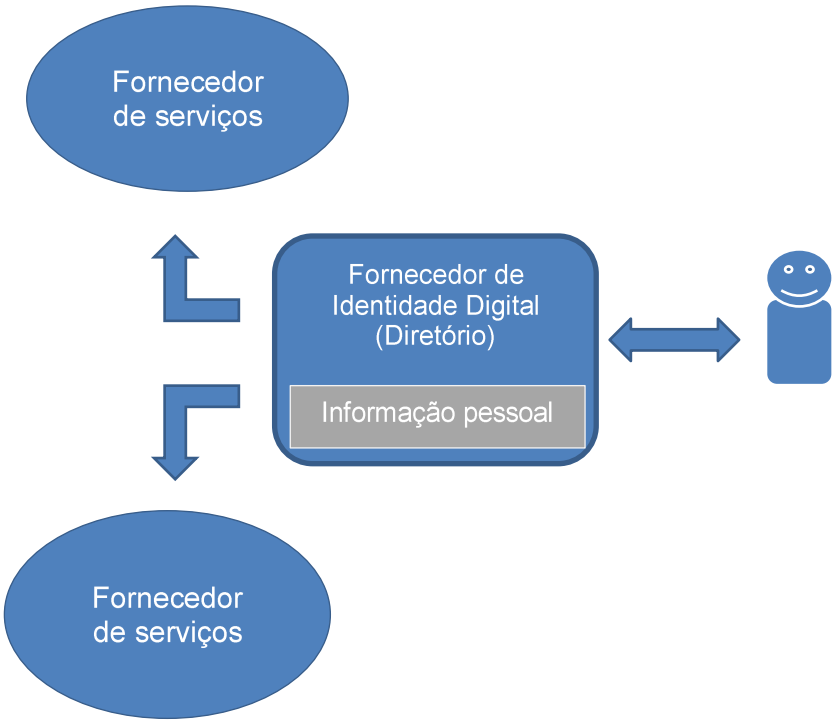


Figura 7 - Sistema Centralizado de Identidade Digital

Sistema Federado de Identidade Digital
Nos sistemas federados, os fornecedores de serviços não agregam a informação das contas dos seus utilizadores, deixando esta tarefa para sistemas específicos que são capazes de agregar múltiplas credenciais (identidades) que são usadas por um utilizador. Este sistema surge como reacção ao desenvolvimento dos sistemas centralizados, que devido à elevada quantidade de informação que agregavam, constituíam problemas legais e de privacidade dos utilizadores.

Nos sistemas federados múltiplos fornecedores de identidade digital, que podem também ser fornecedores de serviços são agregados num ponto central, que se designa *Broker*. Como este *broker* não possui informação específica dos utilizadores, possuindo apenas a capacidade de encaminhar os diferentes pedidos dentro da federação, não constitui um ponto-único de falha, deixando desta forma de ser também um problema em termos legais e de privacidade dos utilizadores. Como vantagem adicional, este tipo de plataforma permite manter os estados de acesso aos serviços (sessões), entre múltiplos fornecedores, o que se torna ideal para plataformas de serviços heterógenas, como referido anteriormente.

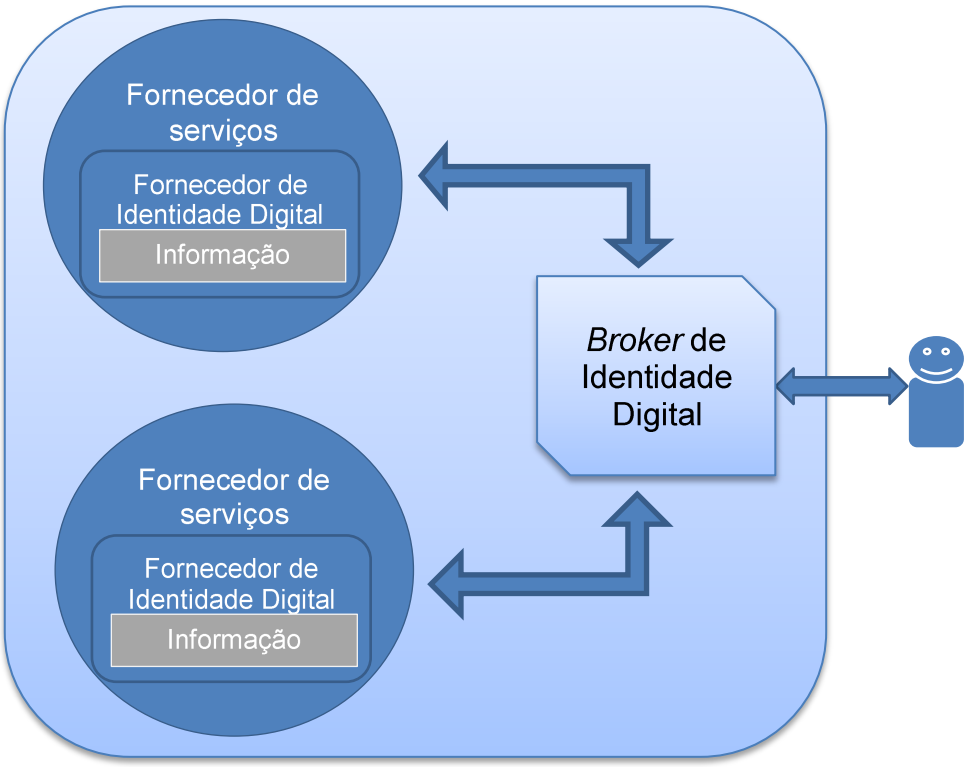


Figura 8 - Sistema de Identidade Digital Federado

Devido a estas características, os sistemas federados passam a ser uma ferramenta fundamental para a partilha de recursos entre organizações, por exemplo, dentro de uma rede de universidades passa a ser possível aceder a recursos que são partilhados por todos os membros do grupo de parceiros – federação. Como a constituição de uma federação tem por base protocolos de colaboração e de confiança, o *broker,* enquanto ponto central da estrutura, pode também possuir capacidade de troca de informação entre diferentes contas dos utilizadores entre parceiros distintos.

Como referido, as federações apresentam um grande conjunto de vantagens relativamente aos sistemas apresentados anteriormente, nomeadamente em plataformas de grande dimensão, no entanto apresentam também novos desafios. Por exemplo, não é fácil a troca de informação entre entidades que não façam antecipadamente parte da federação, o que limita a dinâmica destas estruturas. Adicionalmente é relevante ainda referir que na maioria das federações a informação dos utilizadores, continua a ser detida pelos fornecedores de serviços, e que estes normalmente limitam que esta informação possa ser guardada pelo utilizador para utilização futura – a identidade não é na verdade do utilizador. Esta última questão é muito relevante, pois pode, por exemplo, restringir a liberdade de um utilizador, ou organização, em escolher as entidades que lhe prestam serviço.

Finalmente, sendo os fornecedores de serviços as entidades que detêm a identidade de um utilizador, este pode, em situações limite, deixar de poder ser responsável, ou responsabilizado, pela utilização da sua identidade. Todas as transacções de informação entre o utilizador, o fornecedor de identidade digital, e o fornecedor do serviço, são efectuadas tendo por base declarações (“*claims*”), ou afirmações (“*assertions*”), que transportam os dados de forma segura e normalizada, mas que o detentor da identidade (sujeito) não controla na plenitude.

Sistema de Identidade Digital Centrado no Utilizador
Os sistemas centrados no utilizador têm como principal objectivo dar completo controlo da informação ao utilizador. Por princípio haverá uma separação, e uma maior especificação, dos fornecedores de serviços que são responsáveis pela gestão da identidade digital de um utilizador. Os fornecedores de identidade digital funcionam como uma terceira entidade, que é reconhecida como sendo um agente seguro e de confiança por ambas as partes (utilizador e fornecedor de serviço final). Para além de autenticar um utilizador, estes agentes são também responsáveis por armazenar e partilhar informação do perfil do utilizador. Todas a transacção de informação entre o utilizador, o fornecedor de identidade digital, e o fornecedor do serviço, são efectuadas tendo por base declarações ("*claims*"), ou afirmações ("*assertions*"), que transportam os dados de forma segura e normalizada, mas neste caso, e ao contrário do sistema Federado, o detentor da identidade (sujeito) controla completamente todas as transacções.

Nos sistemas de identidade digital centrados no utilizador, os fornecedores de identidade digital não se encontram dentro de nenhuma federação, comportando-se unicamente como entidade notariais, que certificam a identidade de um determinado utilizador no contexto específico. Como referido, neste tipo de sistema os utilizadores são completamente responsáveis, e consequentemente passiveis de ser responsabilizados, pela informação que transaccionam e pelas consequências dessa transacção de informação.

É importante ainda referir, que neste tipo de sistemas um utilizador pode escolher qual o fornecedor de identidade digital que pretende utilizar em determinado contexto, podendo dessa forma ter informação distribuída de forma segura. Sendo ainda de referir que existe a possibilidade de transferência, entre fornecedores de identidade digital, de toda a informação que o utilizador desejar, desta forma o utilizador passa a ser o verdadeiro detentor da sua identidade.

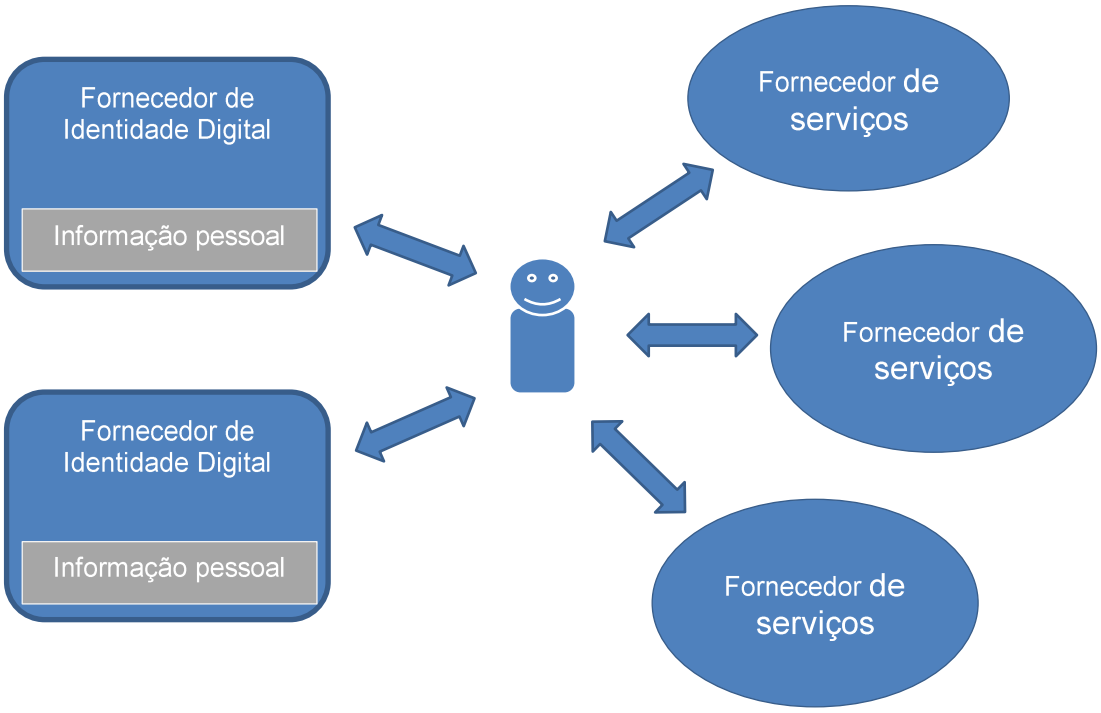


Figura 9 - Sistema de Identidade Digital Centrado no Utilizador

2.3.4 – Modelos Tecnológicos de Referência para plataformas de Identidade Digital

Tendo por base os modelos apresentados anteriormente, e reforçando a importância de se considerarem as necessidades específicas de cada plataforma, por exemplo, de segurança, de dimensão da instalação, entre outras, são apresentados em seguida dois dos modelos tecnológicos considerados no desenvolvimento deste trabalho.

Sistema Centralizado de Identidade Digital – Diretório LDAP

O protocol LDAP (Lightweight Directory Access Protocol) é um protocolo da Internet que permite o acesso por parte de aplicações a informações localizadas num Diretório. Inicialmente baseado no protocolo X.500, desenvolvido pelo ITU-T (International Telecommunication Union - Telecommunication Standardization Sector) em 1988, o LDAP foi desenvolvido com o objectivo de simplificar o acesso aos Diretórios assim como permitir um acesso normalizador, nomeadamente pela utilização do protocolo TCP.

Um Diretório LDAP tem por base a definição de nós (objectos), que agrupam atributos identificados por um nome. Cada atributo, para além de possuir um nome, possui também um identificador único, chamado de OID (Object identifier), sendo que cada OID é único em termos mundiais e é criado segundo as regras também definidos pela especificação ITU-I, Abstract Syntax Notation One (ASN.1), e pelas regras definidas pelo International Standards Organization (ISO). A entidade responsável por garantir o registo dos OIDs de organizações privadas é a Internet Assigned Numbers Authority (IANA).

Para evitar que a estrutura dos diretórios LDAP sejam muito rigidas, é possível a uma organização obter um OID base, sobre o qual desenvolve conjuntos de atributos específicos. No desenvolvimento do Diretório IPP, apresentado na secção 3.2.1, foram criados alguns objectos específicos tendo por base o OID obtido junto da IANA para o Politécnico do Porto.

Cada objecto, ou nó, de um Diretório LDAP possui um conjunto de atributos, por exemplo, um objecto que represente um funcionário numa empresa, deverá possuir atributos como número de telefone, *email*, fotografia, etc. A maioria destes atributos encontra-se normalizada, permitindo por esse motivo um fácil acesso a toda a informação da organização.

Para que seja fácil aceder à informação, um Diretório LDAP é organizado uma estrutura em árvore hierarquizada, e possui ainda um sistema de acesso do tipo cliente-servidor. O protocolo LDAP define: a) o modelo de organização da informação (objectos); b) o protocolo de comunicação entre cliente servidor; c) operações que podem ser executadas sobre a informação (procura, actualização, adição, remoção).

A versão mais recente do LDAP é a versão 3.0 [13], que foi desenvolvida com o principal objectivo de resolver algumas das limitações iniciais do LDAP, em áreas como: internacionalização, autenticação, encaminhamento e implementação.

Em seguida é efectuado um resumo simplificado das diferenças apresentadas, em cada uma das áreas referidas, entre a versão 3.0 do LDAP e a versão 2.0.

	LDAP v2	LDAP v3
Internacionalização	ISO10646	UTF-8 [14] (UCS Transformation Format—8-bit)
Autenticação	Implementa 3 mecanismos: • Anonimo, • Palavra-chave em modo não protegido; • Kerberos v4 [15]	Implementa um mecanismo muito mais versátil baseado na especificação *Simple Authentication and Security Layer* (SASL [16])
Encaminhamento	Permite unicamente o processamento de mecanismos de encaminhamento pelos servidores. Os clientes não são capazes de dar seguimento a mensagens de encaminhamento	Permite que tanto o cliente como o servidor possam processar mensagens de encaminhamento, Com esta alteração passa a ser possível retirar alguma exigência de processamento aos servidores.
Implementação		Possui um conjunto de definições normalizadas, organizados em esquemas [17][18] (*schemas*) onde são agrupados um elevado número de objectos. Desta forma é possível criar estratégias de implementação em larga escala, onde múltiplos diretórios conseguem coexistir na mesma estrutura.

Tabela 1 – Diferenças entre versões de LDAP

Adicionalmente, a versão 3 do LDAP apresenta ainda a possibilidades de serem cridas extensões às funcionalidades base. Uma das extensões mais utilizadas é a extensão StartTLS [19], que define que uma sessão entre o Cliente e o Servidor deverá ser implementada através de encriptação de todos os dados recorrendo ao protocolo TLS (Transport Layer Security).

Um das principais características dos diretórios LDAP é a extrema versatilidade, que é conseguida através da aplicação do conjunto de conceitos apresentado anteriormente. Por fim, é importante referir a enorme facilidade que existe em se alargar o conjunto de definições de objectos atributos que constituem um determinado Diretório. Por esse motivo é fácil encontrar diretórios LDAP na base de sistemas simples, como o que apresenta a figura seguinte, mas também em ambientes muito mais complexos, como o que suporta a estrutura TIC do Politécnico do Porto.

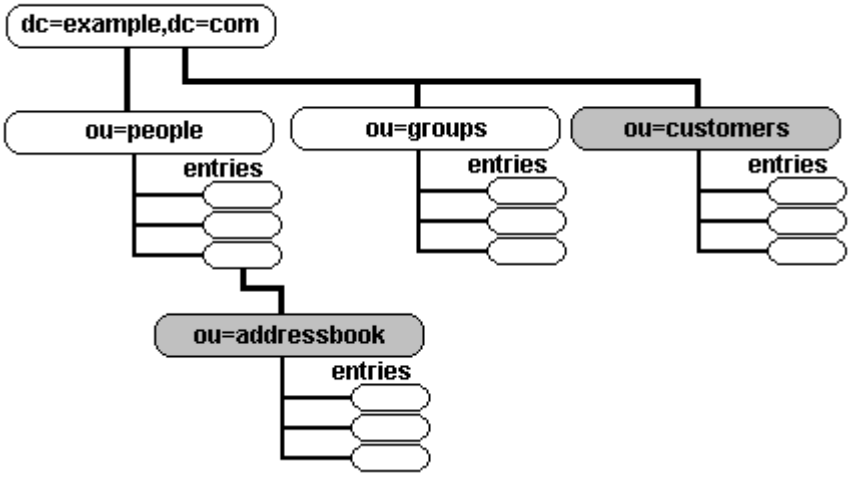


Figura 10 – Estrutura LDAP Simplificada

Como é apresentado na secção 3.2.1, o Diretório do IPP é uma estrutura que suporta informação relativa a toda a estrutura TIC do Politécnico do Porto, nomeadamente informação sobre utilizadores, sobre configurações de equipamentos, sobre configuração e manutenção de sistemas. O desenvolvimento do Diretório IPP foi efectuado durante a execução do projecto IPPwNet.

Sistema Federado de Identidade Digital – Federação SAML

O protocolo SAML [20] (Security Assertion Markup Language) é um protocolo aberto baseado em XML definido pela *Organization for the Advancement of Structured Information Standards* (OASIS). Como modelo de abstração, disponibiliza um conjunto de descrições de declarações e de protocolos para o transporte dessas declarações. É uma linguagem descritiva genérica que permite implementar plataformas de autenticação em ambientes heterogéneos. De forma resumida o modelo definido pelo SAML assenta nos seguintes módulos:

1. Asserções (*Assertions*): Informação sobre autenticação, atributos e autorização;
2. Protocolo: Elementos de pedido e resposta que empacotam as asserções;
3. Vínculos (*Bindings*): Definem como as mensagens do protocolo SAML são usadas dentro de protocolos de transporte (SOAP, HTTP, etc);
4. Perfis (*Profiles*): Como combinar e embeber os diferentes componentes SAML em utilizações específicas – normalização de casos de utilização.

Sendo que a sua relação pode ser definida com a presentado na figura seguinte:

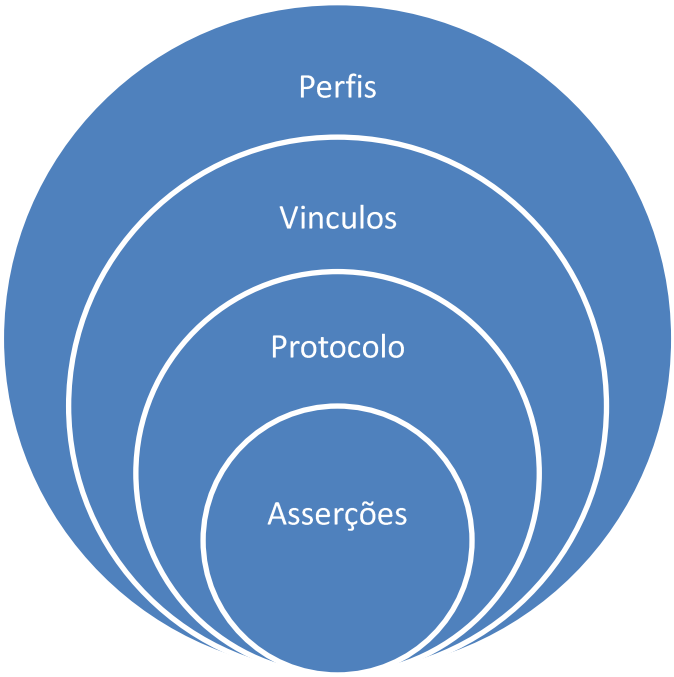


Figura 11 – Componentes SAML

Como referido, o SAML assenta num princípio de abstração, fortalecendo dessa forma a sua principal característica, a versatilidade. Ao contrário de outros mecanismos de autenticação, como é exemplo o OpenID [21], o SAML pode ser aplicado num diversificado conjunto de situações

Em seguida são apresentados de forma resumida as diferentes componentes do modelo SAML.

Asserções (*Assertions*)

As asserções, ou declarações, constituem as unidades atómicas do modelo SAML,

contendo a informação requerida em cada pedido. O modelo XML base para cada asserção é o apresentado no extracto de código seguinte:

```
<saml:Assertion …>
  …
</saml:Assertion>
```

Código 1- Definição base de uma declaração SAML

Tipicamente uma declaração representará a seguinte informação: *Declaração A foi emitida no tempo X, pelo emissor Y, sujeito às condições K.*

De forma resumida o SAML define três tipos de contextos em que as asserções podem ser utilizadas:

- Autenticação (AuthenticationQuery) - pedido de informação sobre um determinado sujeito relativamente ao estado de autenticação, como exemplo: Sujeito A, autenticou-se no instante X, recorrendo ao método Y.
- Autorização (AuthorizationDecisionQuery) – pedido de informação sobre o estado de autorização de um sujeito a um determinado recurso, num determinado instante;
- Atributos (AttributeQuery) – pedido de atributos de um determinado sujeito.

Protocolo

O protocolo base do SAML é simples e baseado num esquema de pergunta (cliente) e resposta (servidor). As perguntas são apresentadas recorrendo a uma formatação XML simples, Já no caso das respostas, estas podem adquirir uma complexidade superior, pois uma resposta pode conter um conjunto de declarações.

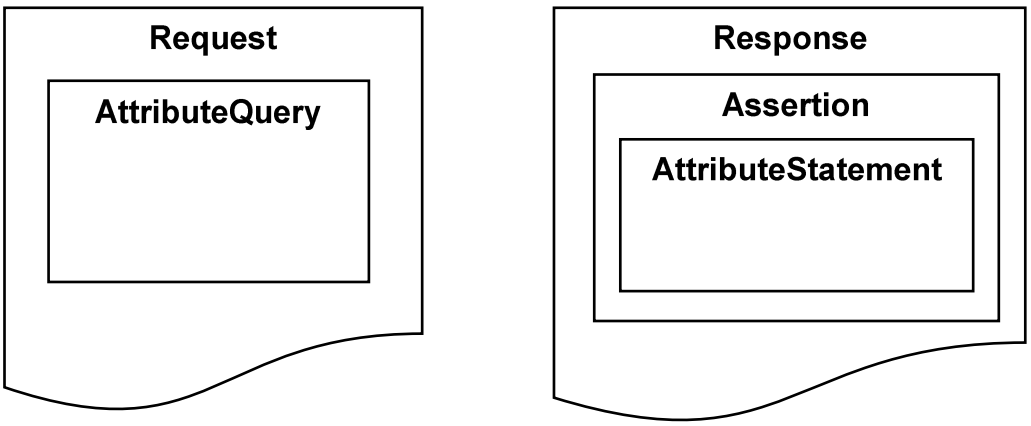


Figura 12 – Protocolo SAML Simplificado

Vinculos (*Bindings*)

Os vínculos definem a forma como o protocolo SAML é utilizado (transportado) sobre outros protocolos, por exemplo o HTTP Redirect, HTTP POST, ou SOAP, Em seguida é apresentado de forma resumida o esquema para o vínculo SOAP [22] (*Simple Object Access Protocol*).

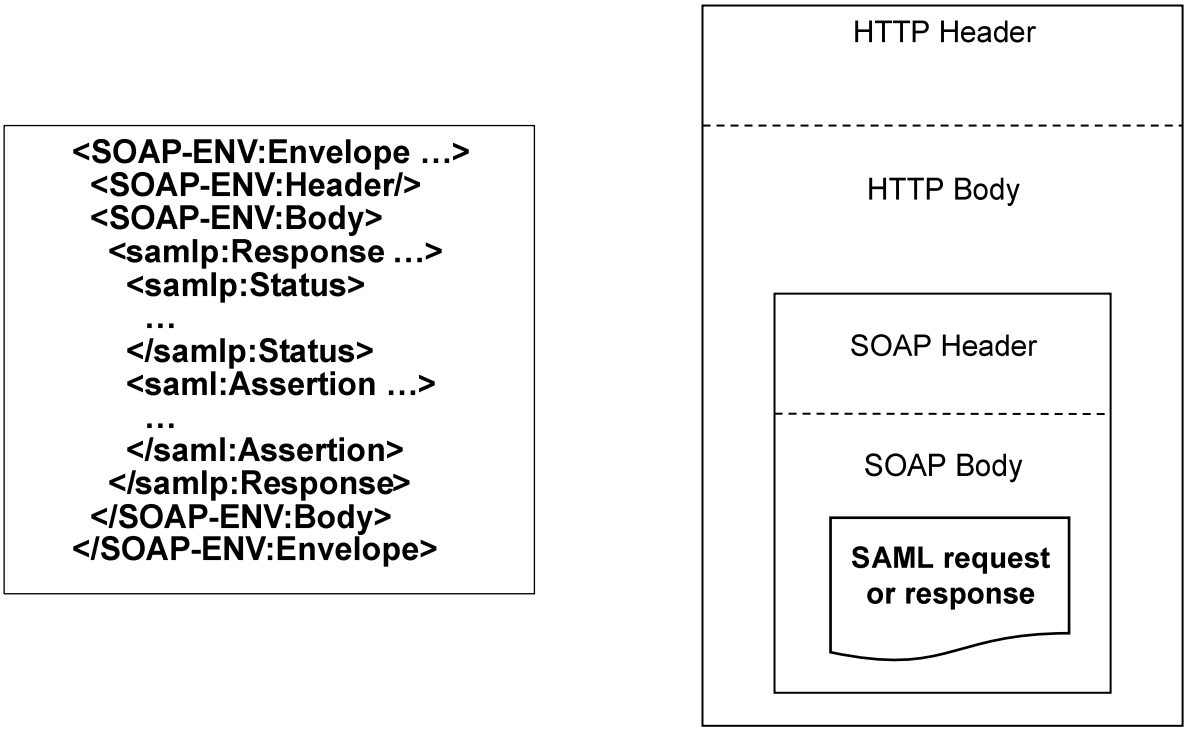


Figura 13 - Vinculo SAML para SOAP

A utilização do protocolo SAML sobre diferentes protocolos de transporto é uma das características que lhe confere a versatilidade referida, permitindo desta forma uma fácil adaptação a um elevado conjunto de situações.

Perfis (*Profiles*)

Os perfis SAML permitem combinar e embeber os diferentes componentes SAML por fim a dar resposta a utilizações específicas. O modelo SAML define ainda dois elementos fundamentais para a definição dos diferentes perfis:

- Fornecedores de identidade (*Identitiy providers* – IdP);
- Fornecedores de serviço (*Service Providers* - SP).

O IdP é responsável por criar, manter e gerir a identidade dos utilizadores, por exemplo tendo como base um Diretório LDAP. Os IdP são também responsáveis por produzir as asserções (*assertions*). Com base nas asserções disponibilizadas pelos IdP os fornecedores de serviços são responsáveis por controlar os acessos aos serviços

De entre os vários perfis de utilização será dado especial enfoque ao perfil “Web Browser SSO” e ao perfil “Single Logout”, pois este é a base para os sistemas de Single-Sign-On utilizadas pelas aplicações Web, e que serviu de base à implementação efectuada neste trabalho. Na figura seguinte é apresentado o diagrama de funcionamento deste perfil.

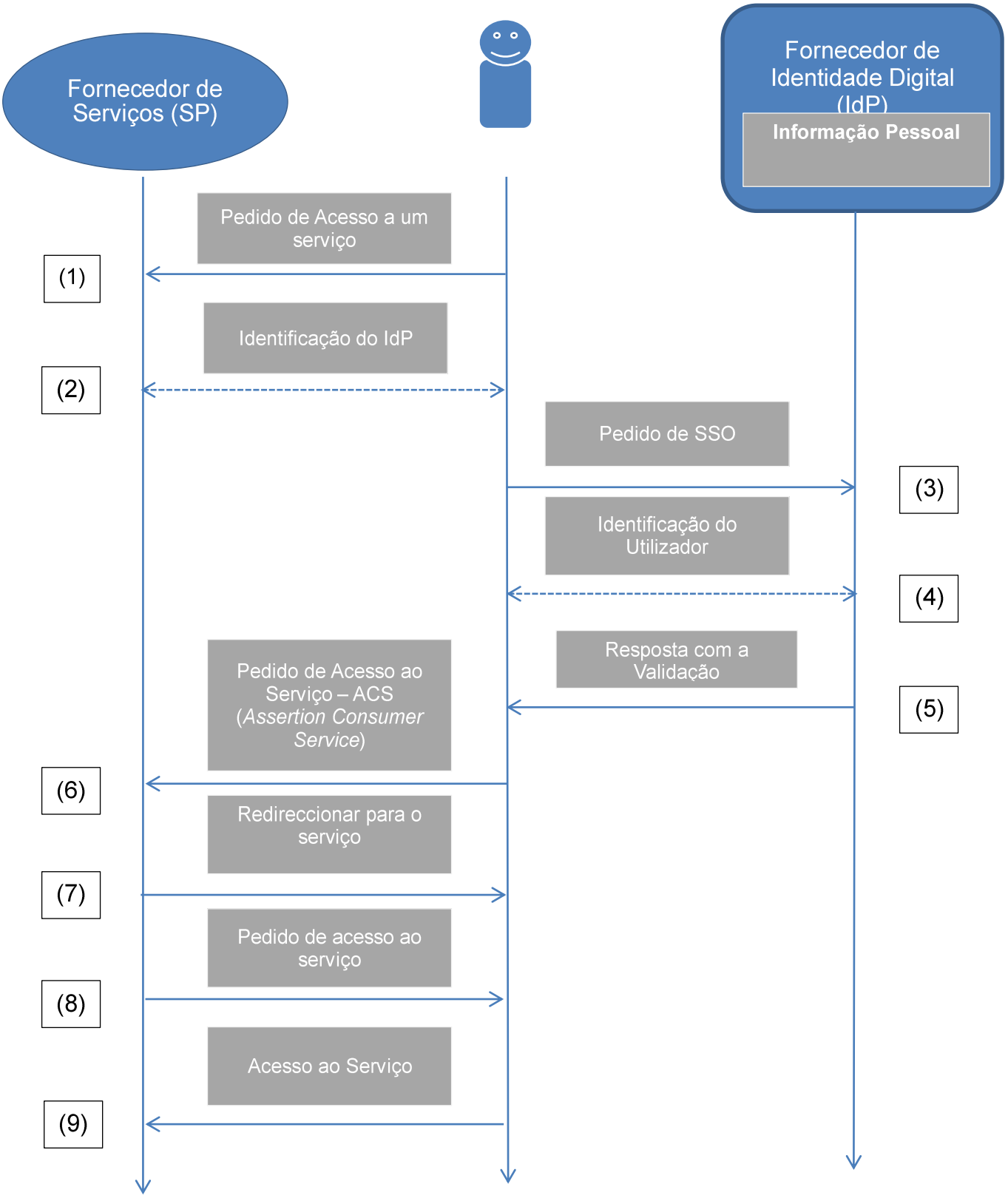


Figura 14 - Perfil SAML Web Browser SSO

3 – Implementação

3.1 – Plataforma de Identidade Digital do Politécnico do Porto – Diretório IPP

Tendo por base a proliferação de sistemas em silo, normalmente associados a novos serviços e aplicações TIC, e ao mesmo tempo, surgindo como resultado de uma evolução quase natural da sua plataforma, o Politécnico do Porto decidiu, no âmbito do projecto IPPwNET, desenvolver uma nova plataforma de identidade digital uniforme para todas as suas unidades.

Esta nova plataforma - Diretório IPP, foi implementada tendo por base um modelo centralizado, como descrito na secção 2.3.4 - "Sistema Centralizado de Identidade Digital – Diretório LDAP". Em seguida é apresentado um esquema da estrutura em árvore do Diretório IPP.

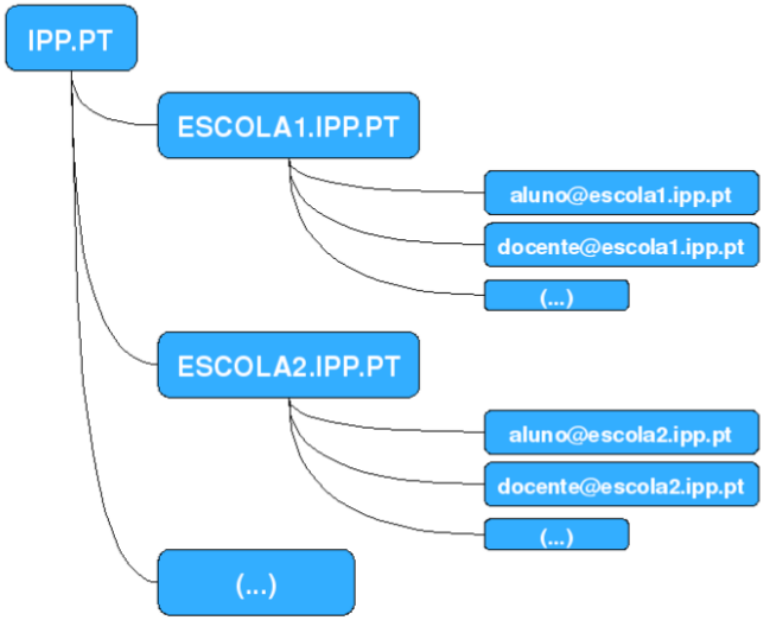


Figura 15 - Estrutura Simplificada do Diretório IPP

3.1.2 - Diretório IPP

O directório IPP é um repositório de informação/recursos dos utilizadores da estrutura informática do IPP. Neste âmbito é responsável pela manutenção e disponibilização de atributos dos utilizadores a todas as aplicações do Sistema de Informação do IPP (Secretaria Virtual, actividade lectiva, sistema de email).
Como tecnologia base de acesso e desenho é utilizado o protocolo LDAP, este permite o armazenamento de dados agrupados em objectos, numa estrutura hierárquica.
Destacamos em seguida algumas das suas características principais:

- Transferência de informação utilizando ligações seguras (TLS/SSL):
- Acesso (autenticação) de utilizadores recorrendo a normas abertas e seguras (SASL);
- Estrutura de replicação em árvore;

- Estrutura de *proxy/cache*;
- Implementação aberta e largamente utilizada;
- Gestão de acessos (ACLS).

O directório IPP implementa as especificações LDAP referidas anteriormente, das quais destacamos as seguintes:

- Ligações seguras (TLS/SSL);
- Autenticação sobre ligações seguras (TLS ou SSL);
- Sistema de replicação em árvore;
- Mecanismo de passagem de autorização.

Como foi referido, o Diretório IPP é construído em árvore e implementa um sistema de replicação de parte ou totalidade dos seus ramos, possui uma base de dados central e uma base de dados por unidade IPP (escola), esta estrutura permite aumentar a disponibilidade e o desempenho do sistema.
Todas as alterações à estrutura devem ser efetuadas diretamente sobre a base de dados central ou então recorrendo, de forma transparente, ao mecanismo de *referral* que o LDAP possui. Este mecanismo permite que um pedido de alteração efetuado numa das replicações, seja reencaminhado para a base de dados central. Como sistema adicional, existe a possibilidade de usar um mecanismo de *proxy/cache*. Por questões de desempenho, a utilização deste mecanismo não é aconselhável e não se encontram atualmente ativo.

O diretório IPP apresenta o seguinte modelo de informação.

Objectos	***Atributos***	***Descrição adicional***
ippNetOrg	o description dn	Unidades IPP
ippNetUser	**Gerais e facultativos** mail audio businessCategory carLicense departmentNumber displayName employeeNumber employeeType givenName homePhone homePostalAddress initials jpegPhoto labeledURI manager mobile pager photo roomNumber secretary userCertificate x500uniqueIdentifier preferredLanguage userSMIMECertificate userPKCS12 **IPPnetEspecificos e facultativos**	Utilizador IPP O atributo ippnetSessionID, utilizado nos mecanismos de passagem de autorização é apresentado no ponto 4 deste documento.

Objectos	*Atributos*	*Descrição adicional*
	ippNetSessionID ippNetUserEmailAliases ippNetUserEmailHomeDirectory ippNetUserEmailMailQuota ippNetUserEmailMailForwardingAddress ippNetUserEmailDeliveryMode ippNetUserEmailDeliveryProgramPath ippNetUserEmailMailReplyText ippNetUserEmailMailHost ippNetUserMecNumber ippNetUserAccountExpirationDate ippNetUserEmailFilter	
ippNetEmailAccount	cn mail uid mailMessageStore homeDirectory userPassword mailAlternateAddress qmailUID qmailGID mailQuota mailHost mailForwardingAddress deliveryProgramPath qmailDotMode deliveryMode mailReplyText accountStatus	Conta de email
ippNetRecoverData	cn ippNetBI ippNetPergunta ippNetResposta	Dados para recuperação de palavra chave

Em seguida é apresentada a descrição pormenorizada dos atributos específicos da ippNet.

Atributo	*Descrição*	*Tipo de dados*
ippNetTipo	Tipo de utilizador	Texto (string): ALUNO, FUNCIONARIO, DOCENTE.
ippNetAccountPerms	Níveis de acesso de um utilizador	Texto: WIFI, EMAIL, PORTAL,VPN
ippNetAccountType	Tipo de conta	Texto:USER,LOCAL,VISITANTE,ACESSO, etc.
ippNetStatus	Estado da conta(permite ou inibe o acesso	Texto (strig): ACTIVO, INACTIVO
ippNetSessionID	Utilizado no mecanismo de controlo de versões.	Texto: md5(userID+IP Real) (Processo descrito no ponto 4)

Modelo de acesso de dados

O modelo de identificação define a estrutura base do directório IPP e a forma como os objectos (recursos) são acedidos. No directório IPP é utilizado um modelo de mapeamento entre os nomes DNS e nomes LDAP. Este modelo é descrito pela RFC2247. De forma resumida esta RFC define o atributo *dc* que identifica uma componente de domínio (*domain component*), define ainda a forma como os nomes DNS são separados para criar as componentes de domino (*dc*).

No directório IPP um objecto existente no domínio DNS: unidade*A.ipp.pt,* terá a identificação LDAP: dc=unidadeA,dc=ipp,dc=pt. Este modelo permite adicionar ao directório IPP a capacidade de disponibilizar e publicar recurso de forma transparente.

No caso dos objectos utilizador (ippNetUser) e para permitir a compatibilização com as estruturas já existentes, são disponibilizados três mecanismos de acesso/identificação:

- nome de utilizador - uid=userA,dc=unidadeA,dc=ipp,dc=pt;
- endereço de correio electrónico email - email=userA@unidadeA.ipp.pt;
- sigla - sigla=userA,dc=unidadeA,dc=ipp,dc=pt.

A verificação da identidade do utilizador é efectuada pelo directório, recorrendo ao atributo *userPassword*

Mecanismo de passagem de autorização – Gestão de sessões

O mecanismo de passagem de autorização (gestão de sessões), permite que um utilizador autenticado e com autorização de utilização de um dos módulos (aplicação) dos sistemas de informação, passe a utilizar um outro modulo, sem necessitar de se autenticar. Este mecanismo utiliza o atributo *ippnetSessionID* de cada utilizador. Em seguida é apresentado o esquema geral de funcionamento.

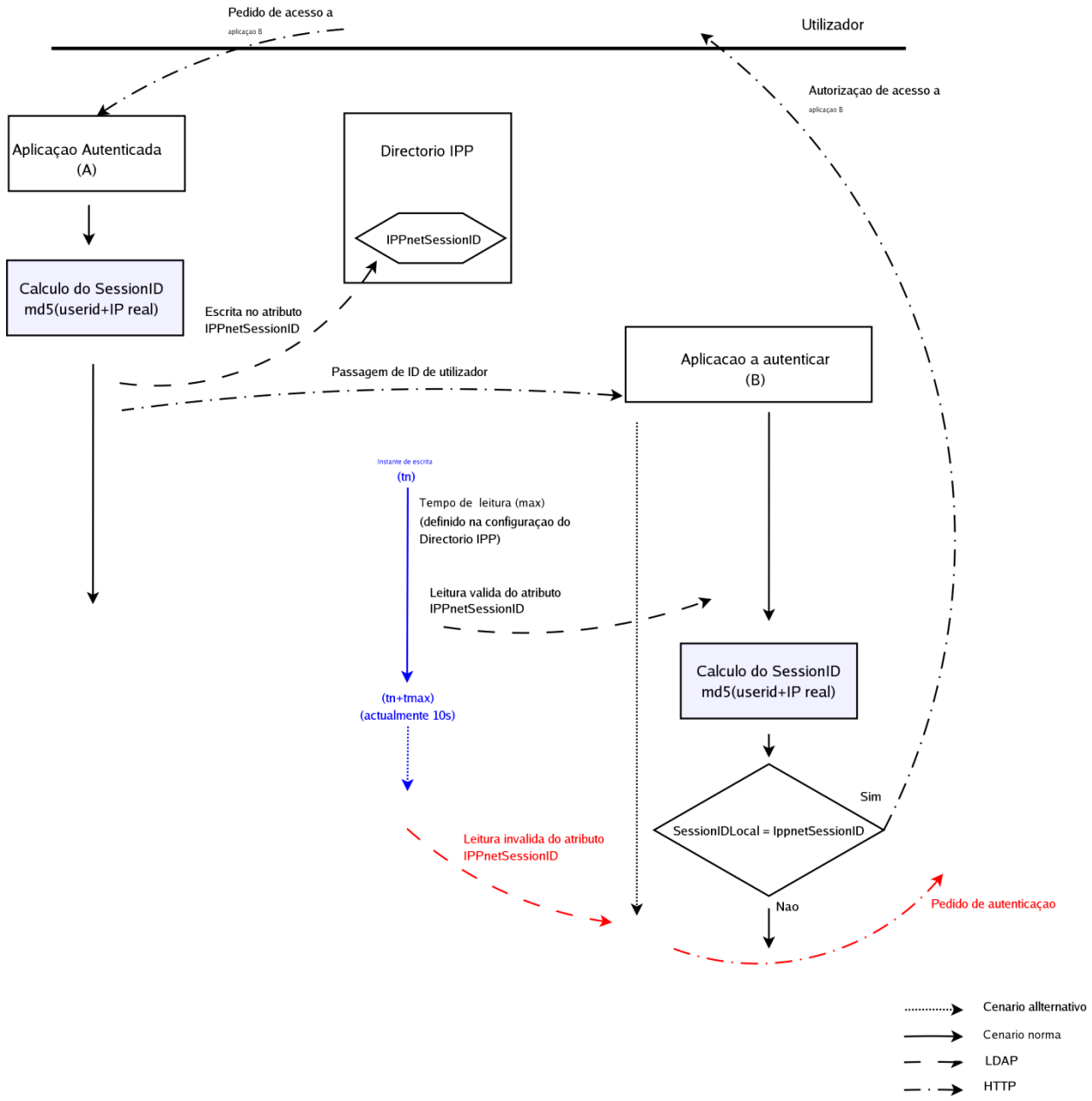


Figura 16 - Mecanismo de passagem de autorização – Gestão de sessões

Para impedir acessos fraudulentos o directório IPP só permite, após cada escrita, uma acção de leitura do atributo *ippnetSessionID* e durante um tempo definido na configuração do servidor, actualmente 10 segundos. A escrita no atributo é unicamente permitida a aplicações autenticadas no perfil do utilizador.

3.2 Plataforma de Identidade Digital do Politécnico do Porto – Modelo Federado

De acordo com o que é apresentado na secção 2.3.3, os modelos centralizados, como o utilizado pelo Diretório IPP, permitem que as organizações tenham enormes ganhos na gestão das suas plataformas TIC, pois, entre outras vantagens, torna-se possível disponibilizar novos serviços e aplicações de forma integrada. No entanto, e em especial no caso de organizações de média e grande dimensão, estes sistemas apresentam problemas de escalabilidade e segurança.

Paralelamente, e no caso do sistema implementado pelo Politécnico do Porto, foi também considerado que a estrutura em árvore, que mapeava a estrutura de dados nas unidades orgânicas, começava a apresentar-se como um entrave ao aparecimento de novos serviços, comuns a todos os alunos, docentes e restantes funcionários.

Tendo por base esta análise foi efectuada a criação de um domínio virtual que suportasse a disponibilização de perfis comuns a todos os utilizadores. Com a criação do domínio virtual tornou-se possível desenvolver os novos serviços, comuns a toda a comunidade do Politécnico do Porto e, dessa forma, alargar o âmbito da plataforma de identidade digital apresentada pelo Diretório IPP.

Na figura seguinte é apresentada a forma como este o domínio virtual se interliga com a estrutura já existente.

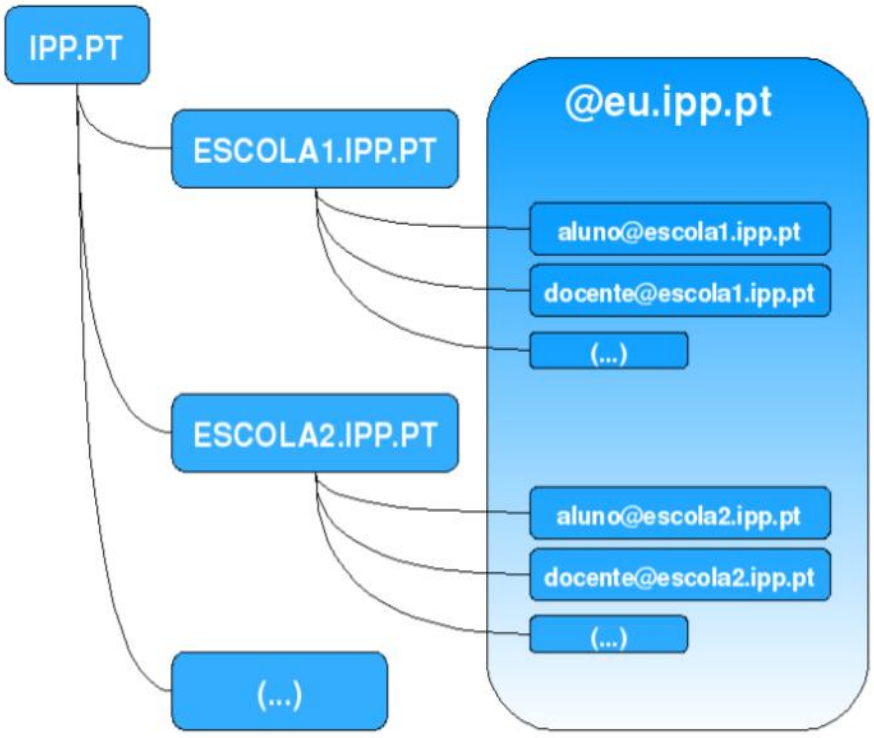


Figura 17 – Domínio virtual EU.IPP.PT

Para além de servir de ligação entre as diferentes unidades do Politécnico do Porto, o domínio EU.IPP.PT pretendia também servir de identificador único para todas as aplicações e serviços. Na figura seguinte é apresentada de forma simplificada a integração planeada para o domínio virtual EU.IPP.PT.

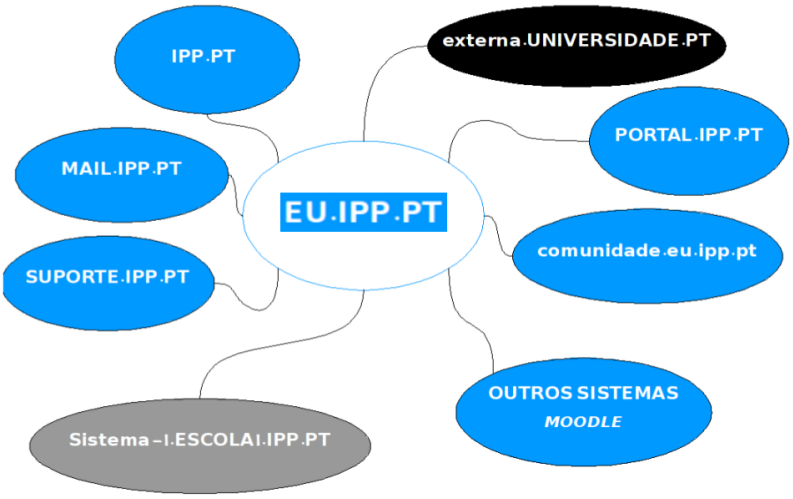


Figura 18 - Diagrama da Plataforma de Identidade Digital do IPP

Com o objectivo de implementar a estratégia apresentada com a criação do novo domínio virtual, considerou-se fundamental complementar o modelo da plataforma de identidade digital baseado no Diretório IPP para o modelo federado, aumentando ao mesmo tempo a segurança e desempenho do sistema.

No seguimento da análise efectuada na secção 2.3.4, a plataforma proposta e desenvolvida no âmbito deste trabalho, para complementar o desenvolvimento efectuado, tem por base a implementação do protocolo SAML versão 2.0, e o perfil *Web Browser SSO,* também descrito na sessão 2.3.4. A versão 2.0 do SAML, para além de apresentar uma evolução clara relativamente à versão anterior, possui ainda uma enorme aceitação por parte da maioria dos fabricantes de serviços Cloud Computing, como são o caso do Google, Microsoft, entre outros.

Neste sentido, pretendeu-se que a plataforma desenvolvida responda aos problemas identificados e, ao mesmo tempo, permita ainda criar as condições para concretizar com êxito o principal objectivo deste trabalho - desenvolver uma plataforma de identidade digital capaz de impulsionar a adopção dos novos modelos de governação TIC, nomeadamente, o modelo apresentado pele Cloud Computing.

O desenvolvimento de uma plataforma de raiz baseada em SAML 2.0 demonstrou-se como necessário, pois à data do início do projecto não existiam soluções robustas no mercado que implementassem esta nova norma. Foi ainda estudado a possibilidade de recorrer a plataformas de identidade digital baseadas na norma 1.1 do SAML, no entanto, e como referido, a versão 1.1 da norma não possuía algumas das características consideradas fundamentais para o desenvolvimento da plataforma pretendida. De entre algumas dessas características destacamos as seguintes:

- Falta de encriptação e de assinatura digital das mensagens;
- Inexistência de mecanismos para terminar sessões (efectuar *logout*);

- Inexistência de mecanismos de mapeamento entre atributos, por exemplo com servidores LDAP, etc.

Considerando a necessidade de desenvolver uma plataforma que permitisse uma implementação ágil, e ao mesmo tempo uma manutenção fácil, todo o trabalho foi desenvolvimento utilizando o *framework* de programação Ruby On Rails. Considerando ainda a importância de tornar o sistema aberto a novas funcionalidades, todo o desenvolvimento foi efectuado recorrendo a uma estrutura modular, apresentada e descrito de forma global em seguida.

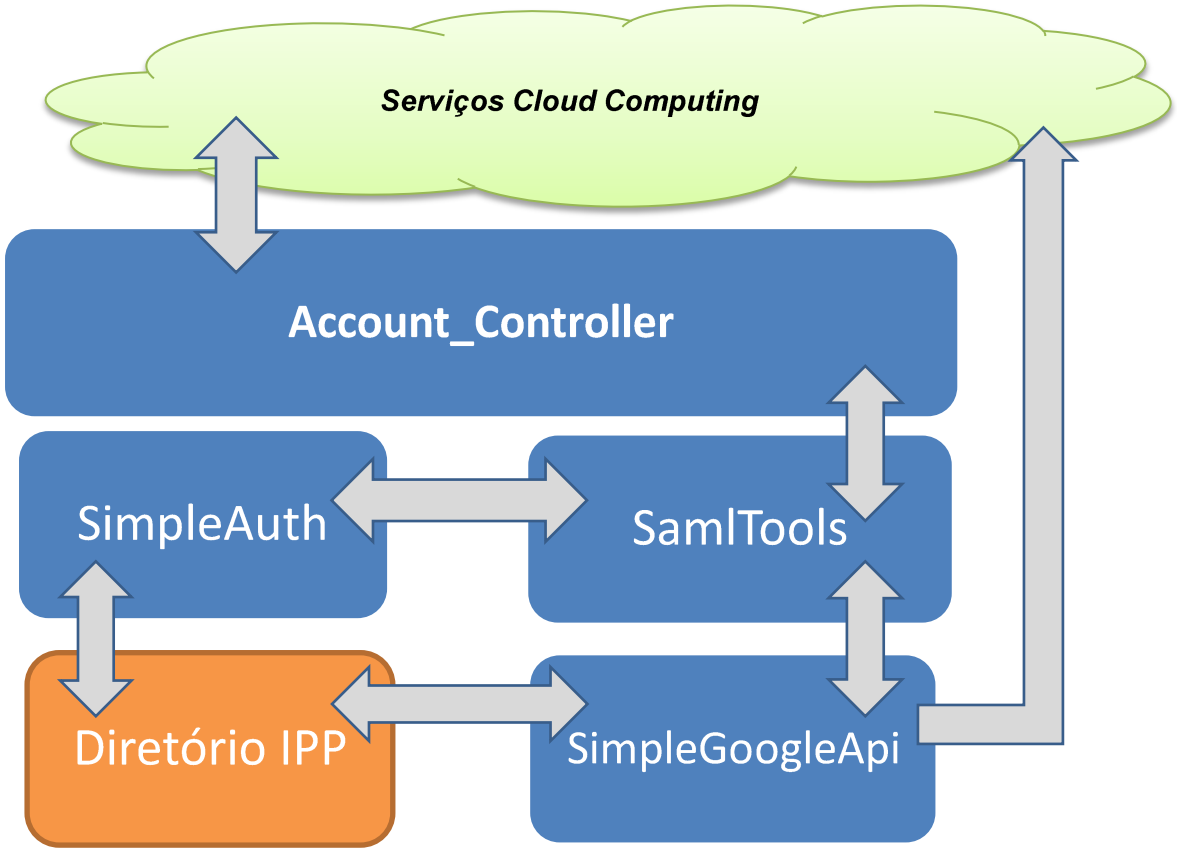


Figura 19 – Plataforma de identidade digital do Politécnico do Porto – Modelo Federado

Account_Controller
Este módulo apresenta-se como o núcleo principal da aplicação. Para além de implementar os mecanismos de Login e Logout definidos pela norma SAML, possui ainda as funções básicas de interface com o utilizador.

Em seguida é apresentado um extracto do código de inicialização do módulo.

```
require 'components/saml_tools'
require 'components/simple_g_api'
require 'components/simple_auth_tools'
require 'net/http'
require "ldap"

class AccountController < ApplicationController

  MAX_SESSION_TIME = 120 * 60

  before_filter :check_authentication, :except => [:login, :login_form, :comunidade_info, :comunidade_m_info]

  layout "account_layout", :except => [:logout]
```

Código 2- Inicialização do módulo Account_Controller

No código apresentado é possível verificar a utilização dos diferentes módulos desenvolvidos no âmbito deste projecto, nomeadamente o módulo de implementação da especificação SAML, o módulo de interface com o API do Google e o módulo de autenticação.

SimpleAuth

O módulo SimpleAuth possui as funcionalidades de ligação entre os perfis SAML e os atributos de autenticação existentes em plataformas em silo, como são o caso do LDAP, ou então de sistemas RADIUS. Na implementação actual, e apesar de o módulo estar desenhado para suportar outros módulos de utilização, só foi implementado os mecanismos de autenticação em diretórios LDAP.

No código apresentado em seguida é demostrada a utilização do módulo Simple Auth para validação da identidade de um utilizador. A implementação efetuada permite uma abstração da complexidade específica de cada processo de autenticação (LDAP, RADIUS, etc). No extracto de código nº3 é apresentado um exemplo de autenticação LDAP (3.1) e o processo de colocação dos dados do pedido SAML são mantidos em cache (3.2).

```
(3.1)  user = SimpleAuth::LdapAuth.new()
         begin
          user.set_id(user_id)
          user.pass=pass
           if user.login then
           ser_dn=user.dn
             log("User Logged in, valid user_id(#{user_id}) and pass; User dn=#{user_dn}")
             session[:username] = user.cn
             session[:user_id] = user_id
             if session[:intended_action].nil? or session[:intended_action].include?("login_form") then
                 redirect_to :action => ""
             else
               flash.keep
                          redirect_to :action => session[:intended_action]
             end
          else
             flash[:error] = "Não foi possivel validar a identidade do utilizador apresentado."
             log("Não foi possivel validar a identidade do utilizador apresentado:#{user.id}"  + user.error_msg)
             #flash.keep
(3.2)         flash.keep(:saml_request)
              flash.keep(:saml_relay_state)
              flash.keep(:saml_http_method)
             redirect_to :action => "login_form"
            return
          end
```

Código 3 – Utilização do módulo SimpleAuth para acesso a um servidor LDAP

No código apresentado no exemplo nº4 é detalhado o processo de login no diretório LDAP (4.1). Este processo é originado num sub-processo de procura do nó correspondente ao utilizador a ser autenticado (4.2). A autenticação final do utilizador é efetuada como apresentado na secção anterior.

```
def login()
  begin
    connect_server(@@servers[@@server_index].ip)
    if not auth?(@@servers[@@server_index].access_user,@@servers[@@server_index].access_pass) then
      raise SimpleAuth::RuntimeException, "Unable to access Auth server: #{@@servers[@@server_index].ip}"
    end
    @find_entry = false
(4.2)  @conn.search( @@base_dn, LDAP::LDAP_SCOPE_SUBTREE, "#{@@index_attr}=#{@id}","mail") do |entry|
      @id=""
      if not @find_entry then
        @find_entry= true
        @id = entry.get_dn
        @dn = entry.get_dn
      else
        raise SimpleAuth::RuntimeException, "Invalid number of entries for the given index attr (#{@@index_attr})"
      end
    end
    @conn.unbind if @conn.bound?
   rescue LDAP::ResultError => msg
    @error_msg << "Unable to access Auth server: #{@@servers[@@server_index].ip}" << msg
    raise SimpleAuth::RuntimeException, "Unable to access Auth server: #{@@servers[@@server_index].ip}" << msg
   end

  @conn.unbind if @conn.bound?
  return(false) if @id.empty? or not @find_entry
(4.1)  return(true) if auth?()
 nd
```

Código 4 –– Implementação da função de login pelo módulo SimpleAuth

SamlTools

Este módulo implementa as funcionalidades básicas da especificação SAML 2.0, nomeadamente os mecanismos de autenticação recorrendo ao perfil "Web Browser SSO" descrito na secção 2.3.4. Adicionalmente este módulo implementa ainda um conjunto de funções de suporte, como por exemplo, a encriptação e assinatura de mensagens XML.

No extracto de código apresentado em seguida é detalhado o processo de obtenção dos atributos de uma sessão SAML utilizando o módulo SamlTools. O processo começa pela descodificação (5.1) dos elementos SAML, e em seguida pela obtenção dos elementos XML (5.2) contidos na mensagem SAML.

```
    saml_bind = SamlTools::SamlBindHTTPRedirect.new(@saml_request)
(5.1) @saml_xml= saml_bind.decode()
    parser_tree = REXML::Document.new(@saml_xml)
    #getting request params
    @saml_consumer_service_url = parser_tree.root.attributes["AssertionConsumerServiceURL"]
    @saml_issue_instant = parser_tree.root.attributes["IssueInstant"]
(5.2) @saml_issue_request_id = parser_tree.root.attributes["ID"]
    @saml_provider_name = parser_tree.root.attributes["ProviderName"]
    @saml_issuer = parser_tree.root.elements["saml:Issuer"].text()
    @saml_name_id_policy = parser_tree.root.elements["samlp:NameIDPolicy"].attributes["Format"]
```

Código 5 - Descodificação das mensagens SAML e obtenção de atributos utilizando o módulo SamlTools

SimpleGoogleAPI
Este módulo foi desenvolvido com o objectivo de implementar algumas das funcionalidades de gestão da plataforma Google APPs, nomeadamente de adição remoção e edição de utilizadores. É um módulo complementar usado para o desenvolvimento da plataforma de teste.

No extracto de código seguinte é apresentado um exemplo de utilização do módulo SimpleGoogleAPI para criação de um utilizador na plataforma GoogleApps. Por forma a simplificar a implementação, o módulo possui uma componente integrada de customização do código XML (6.1) que contem os atributos do utilizador. A interação com o serviço do Google é implementada através de um processo REST[24] (6.2).

(6.1)
```
user_add_xml="<?xml version=\"1.0\" encoding=\"UTF-8\"?>"+
"<atom:entry xmlns:atom=\"http://www.w3.org/2005/Atom\" xmlns:apps=\"http://schemas.google.com/apps/2006\">"+
"<atom:category scheme=\"http://schemas.google.com/g/2005#kind\" term=\"http://schemas.google.com/apps/2006#user\"/>"+
"<apps:login userName=\"#{u_id}\" password=\"#{u_i_pass}\" suspended=\"false\"/>"+
"<apps:quota limit=\"2048\"/>"+
"<apps:name familyName=\"#{u_l_name}\" givenName=\"#{u_f_name}\"/>" +
"</atom:entry>"
```

(6.2)
```
if not @@auth_token.nil? or not @@auth_token.empty? then
   headers = {
    'Content-Type' => 'application/atom+xml',
     'Authorization' => "GoogleLogin auth=#{@@auth_token}"
    }
else
   get_token()
   headers = {
     'Content-Type' => 'application/atom+xml',
      'Authorization' => "GoogleLogin auth=#{@@auth_token}"
    }
end
data = user_add_xml
r_response = Simple_g_api.post("www.google.com","/a/feeds/#{domain}/user/2.0",data,headers)

if r_response.is_a?(Net::HTTPSuccess) then
     log("New user (#{user_id}) successfuly created")
     true
else
    @error="Error creating new user (#{user_id})" + r_response.body.to_s
     log(@error)
     false
```

Código 6 – Adição de um utilizador à plataforma do Google utilizando o SimpleGoogleAPI

3.3 – Plataforma de teste – Comunidade.EU.IPP.PT

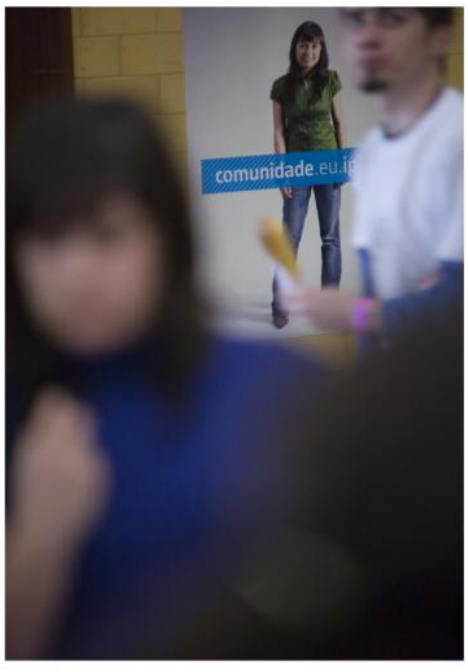
Com o objectivo de testar a plataforma de identidade digital desenvolvida, e de ao mesmo tempo estudar o impacto que os serviços TIC suportados pelo modelo de Cloud Computing podem vir a ter na estratégia do Politécnico do Porto, foi desenvolvida a plataforma de teste COMUNIDADE.EU.IPP.PT. No sentido de aumentar o impacto das TIC na organização, esta plataforma pretende ainda contribuir para os seguintes objectivos:

- Capitalizar novas potencialidades da Internet
- Fomentar a partilha de informação e a cooperação
- Fomentar a inovação
- Dinamizar a formação
- Potenciar a identidade do Politécnico do Porto

Considerando a utilização que as ferramentas desenvolvidas pelo Google possuem na comunidade do Politécnico do Porto, e considerando ainda o facto de estas ferramentas serem disponibilizadas de forma gratuita para as comunidades académicas, foi proposto que a plataforma de testes fosse desenvolvida tendo como base a aplicação Google Apps para a educação. Na decisão de escolha da plataforma do Google, foi ainda determinante o facto de a plataforma Google Apps suportar a autenticação de utilizadores tendo por base o protocolo SAML 2.0, com especificado na sessão 2.3.4, e como é implementado pela plataforma de identidade digital do Politécnico do Porto.

No seguimento da estratégia apresentada com a criação do domínio virtual EU.IPP.PT, e ainda no seguimento da grande aceitação que a plataforma teve, foi decidido desenvolver uma imagem de integração de toda a comunidade do Politécnico, promovendo ao mesmo tempo a utilização da plataforma de Identidade Digital desenvolvida. Na imagem seguinte é apresentada um resumo da campanha efetuada.

comunidade



Como referido, a plataforma da Comunidade do Politécnico do Porto é baseada na ferramenta do GoogleApps, permitindo uma perfeita integração em termos de imagem e de funcionalidades. Na imagem seguinte é apresentado o aspecto da página de entrada, após a validação da sessão.

Figura 20 – Plataforma Comunidade.EU.IPP.PT

Com objectivo de permitir uma fácil utilização, a plataforma de identidade digital desenvolvida possui uma página de acesso customizada, assim como uma página de início de sessão. Nas duas imagens seguintes é feita uma apresentação destas duas características.

Figura 21 – Página de pedido de credenciais de acesso na plataforma

Figura 22 – Página de controlo e verificação de sessão

4 – Resultados de utilização

A criação da plataforma COMUNIDADE.EU.IPP.PT permitiu estudar a implementação SAML efectuada em termos de desempenho e qualidade do código desenvolvido. Como é possível verificar pelos dados de utilização apresentados nos gráficos seguintes, a implementação SAML desenvolvida no âmbito deste trabalho mostrou-se extremamente estável e escalável, não tendo sido necessário qualquer desenvolvimento de suporte ou correcção de erros durante o período de testes. É ainda importante referir a forte utilização que a plataforma possui, sendo de salientar o mais de meio milhão de autenticações com sucesso que a plataforma teve, assim como o elevado número de registos que são efectuados no início de todos os anos lectivos do período de teste.

Nas figuras seguintes são apresentados alguns gráficos de utilização da plataforma.

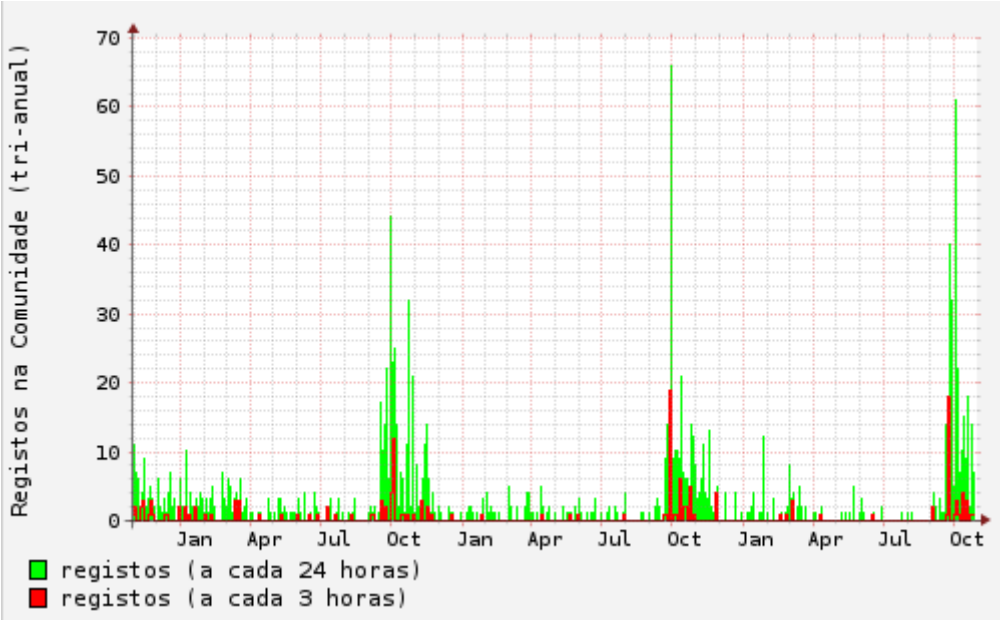


Figura 23 – Número de utilizadores registados durante os últimos três anos lectivos (2010, 2011, 2012)

Neste gráfico é possível mostrar o número de utilizadores que são criados, com especial relevo para os novos utilizadores criados no início de cada ano lectivo, o que corresponde a cerca de 70 utilizadores criados por dia neste período.

Os gráficos seguintes mostram o número de utilizadores autenticados com sucesso. Estes dois gráficos tornam possível verificar que o sistema se mostrou muito estável durante todo o período de testes, não tendo sido verificado nenhuma interrupção do serviço.

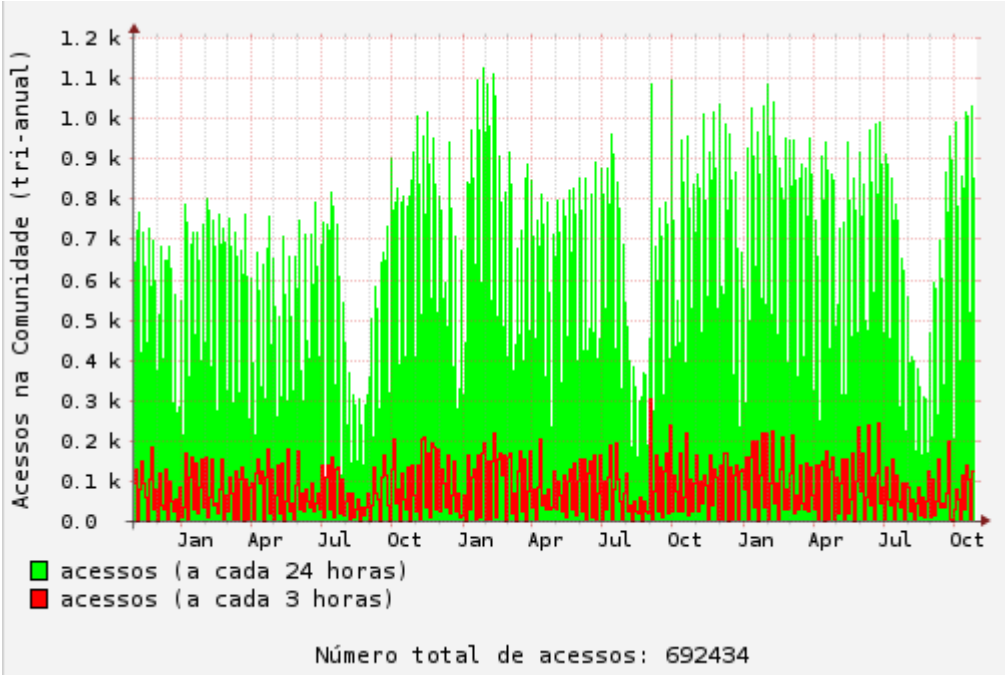


Figura 24 – Número de autenticações com sucesso efectuadas pela plataforma

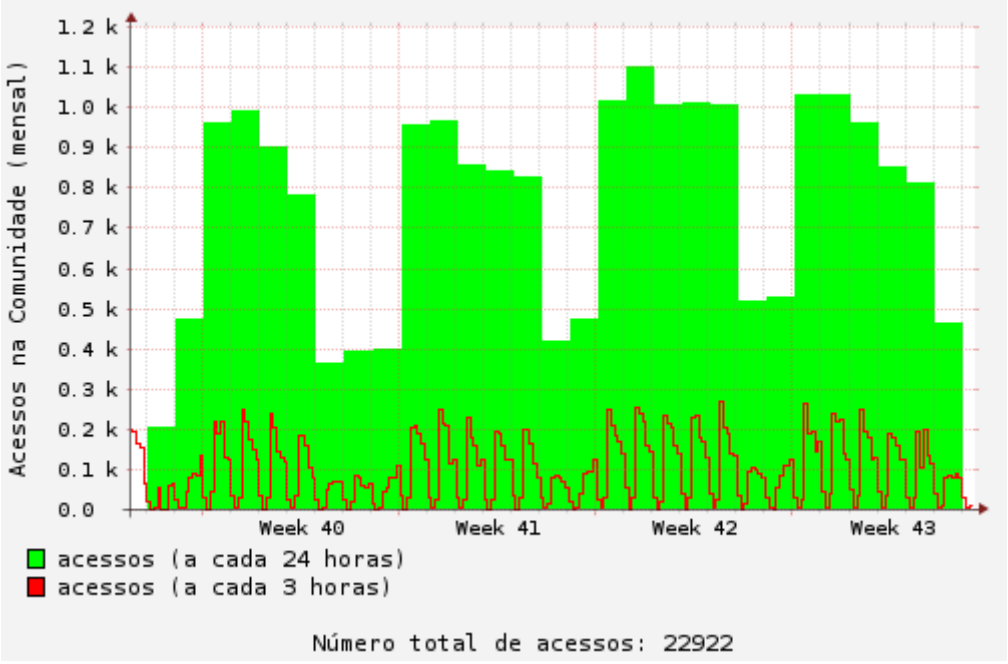


Figura 25 – Número de autenticações com sucesso por mês

5 – Conclusões Trabalhos Futuros

Analisando os resultados que foram obtidos, e que entretanto foram sendo apresentados no decorrer deste relatório, é possível concluir que a estratégia aplicada permitiu atingir com sucesso os objectivos inicialmente propostos. A plataforma de Identidade Digital desenvolvida demonstrou ser de fácil utilização, segura e muito robusta.
A qualidade do trabalho agora apresentado e a experiência conseguida durante a sua realização, permitiram ainda a participação de forma muito ativa no desenvolvimento da plataforma de AAI (Autenticação Autorização e Identidade) promovida pela Fundação para a Computação Cientifica Nacional (FCCN).

O impacto das acções de disseminação dos resultados, nomeadamente o sucesso da primeira edição da conferência CloudViews[1], organizada no decorrer deste trabalho e que contou com mais de 200 participantes, permite ainda concluir que a estratégia implementada tem um alcance internacional, ultrapassando inclusive aquilo que eram os objectivos iniciais.

Como trabalhos futuros é importante referir que o trabalho implementado pode ser desenvolvido para suportar mais sistemas de bases de dados de utilizadores, como por exemplo sistemas RADIUS. Considera-se ainda que é importante desenvolver os sistemas que constituem a plataforma TIC do IPP, como por exemplo os portais académicos, e a secretaria electrónica, para que passem a usar o sistema de identidade digital desenvolvido, pois desta forma vão poder fazer parte da federação de serviços que a FCCN suporta. Esta integração permitira ainda partilhar algumas das funcionalidades apresentadas pela ComunidadeEU.IPP.PT e pelas ferramentas do Google.

[1] http://2009.cloudviews.org

6 - Bibliografia e referências

[1] The rise of the networked enterprise: Web 2.0 finds its payday, Jacques Bughin and Michael Chui, McKinsey Global Institute
[2] How companies are benefiting from Web 2.0, McKinsey&Company
[3] http://cordis.europa.eu/fp7/ict/security/docs/the-cloud-understanding-security-privacy-trust-challenges-2010_en.pdf
[4] http://europa.eu/rapid/press-release_IP-12-1025_en.htm?locale=en
[5] http://europa.eu/rapid/press-release_SPEECH-12-38_en.htm
[6] https://cio.gov/wp-content/uploads/downloads/2012/09/Federal-Cloud-Computing-Strategy.pdf
[7] http://www.finance.gov.au/e-government/strategy-and-governance/docs/final_cloud_computing_strategy_version_1.pdf
[8] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
[9] P. J. Windley, Digital Identity: Unmasking Identity Management Architecture. Sebastopol, CA: O'Reilly, 2004,
[10] http://tools.ietf.org/html/rfc4510
[11] http://tools.ietf.org/html/rfc4512
[12] http://www.itu.int/ITU-T/studygroups/com17/languages/X.680-0207.pdf
[13] http://www.ietf.org/rfc/rfc2251.txt
[14] http://www.ietf.org/rfc/rfc2279.txt
[15] http://www.kerberos.org/about/index.html
[16] http://www.ietf.org/rfc/rfc2222.txt
[17] http://www.ietf.org/rfc/rfc2256.txt
[18] http://www.ietf.org/rfc/rfc2252.txt
[19] http://www.rfc-editor.org/rfc/rfc2830.txt
[20] http://saml.xml.org/saml-specifications
[21] http://openid.net/specs/openid-authentication-2_0.html
[22] http://www.w3.org/TR/soap/
[23] http://rubyonrails.org/
[24] http://tools.ietf.org/html/draft-griffin-bliss-rest-00
[25] http://www.google.com/enterprise/apps/education/