Universidade de Aveiro
2015
Departamento de Eletrónica, Telecomunicações e Informática

Hélder José Rodrigues Gomes

Serviços Orientados a Eventos da Vida Controlados pelo Cidadão

Universidade de Aveiro
2015

Departamento de Eletrónica, Telecomunicações e Informática

Hélder José Rodrigues Gomes

Serviços Orientados a Eventos da Vida Controlados pelo Cidadão

Tese apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Doutor em Engenharia Informática, realizada sob a orientação científica do Prof. Doutor João Gonçalo Gomes de Paiva Dias, Professor Coordenador da Escola Superior de Tecnologia e Gestão de Águeda da Universidade de Aveiro e do Prof. Doutor André Ventura da Cruz Marnoto Zúquete, Professor Auxiliar do Departamento de Eletrónica, Telecomunicações e Informática da Universidade de Aveiro.

Apoio financeiro da FCT no âmbito do Programa de Apoio à Formação Avançada de Docentes do Ensino Superior Politécnico (PROTEC) (Ref. SFRH/BD/49849/2009)

Para a Li e para a Mariana.

o júri

presidente

Prof. Doutor Carlos Alberto Diogo Soares Borrego
Professor Catedrático do Departamento de Ambiente e Ordenamento da Universidade do Aveiro

Prof. Doutor Joaquim Arnaldo Carvalho Martins
Professor Catedrático do Departamento de Eletrónica, Telecomunicações e Informática da Universidade de Aveiro

Prof. Doutor Carlos Nuno da Cruz Ribeiro
Professor Associado do Departamento de Engenharia Eletrotécnica e de Computadores do Instituto Superior Técnico da Universidade de Lisboa

Profª Doutora Delfina Fernanda Moreira Garcês de Sá Soares
Professora Auxiliar do Departamento de Sistemas de Informação da Escola de Engenharia da Universidade do Minho

Prof. Doutor Luís Filipe Coelho Antunes
Professor Associado do Departamento de Ciências da Computação da Faculdade de Ciências da Universidade do Porto

Prof. Doutor João Gonçalo Gomes de Paiva Dias
Professor Coordenador da Escola Superior de Tecnologia e Gestão de Águeda da Universidade de Aveiro (Orientador)

agradecimentos

Aos meus orientadores, o Prof. Doutor Gonçalo Paiva Dias e o Prof. Doutor André Zúquete pela sua permanente disponibilidade, pelas suas críticas e sugestões e sobretudo pela confiança e permanente incentivo, que na etapa final foram decisivos.

À direção da Escola Superior de Tecnologia e Gestão de Águeda (atual e anterior), pela criação das condições que permitiram a realização deste trabalho.

Aos meus colegas da ESTGA, e sobretudo ao grupo de Informática, pelo seu incentivo, destacando ainda o Fábio, o Ciro e o David, meus colegas de gabinete, pelo interesse demonstrado, pelo incentivo e pelas frequentes e enriquecedoras conversas sobre o tema deste trabalho e muitos outros.

Aos meus pais, que criaram as condições para que eu trilhasse o caminho que me permite estar hoje aqui.

Um agradecimento especial à minha esposa, a Li, e à minha filha, a Mariana, pela imensa paciência e compreensão pelas minhas inúmeras ausências durante estes anos e sobretudo porque apesar disso mantiveram um constante apoio e incentivo.

Finalmente, a todos os restantes familiares e amigos porque, de uma forma ou de outra, todos contribuíram para o resultado final deste trabalho.

palavras-chave

eventos da vida, e-government, prestação de serviços de governo eletrónico, agregação de documentos, privacidade

resumo

A progressiva introdução das Tecnologias da Informação e Comunicação na Administração Pública (AP) provocou uma grande evolução na prestação de serviços ao cidadão. Transitou-se de um paradigma de prestação de serviços baseado nas competências de cada instituição, resultado da organização da AP em silos, para um paradigma de prestação de serviços integrados, que pode envolver a participação de serviços de várias instituições, que para o efeito trocam informação entre si, porventura sem que o cidadão disso se aperceba. Um dos objetivos da integração de serviços é a prestação de serviços que visam satisfazer situações do dia-a-dia do cidadão que implicam a interação com serviços da AP, i.e., serviços orientados a eventos da vida (serviços OEV). No entanto, apesar da bondade do objetivo, a integração de serviços é complexa e tem o potencial para criar situações desfavoráveis para o cidadão, nomeadamente para sua privacidade. Com efeito, o cidadão deixa de ter o controlo sobre a difusão da sua informação pelas várias instituições, uma vez que são estas que comunicam entre si para obter a informação necessária para a prestação dos respetivos serviços.

Nesta tese propomos um modelo de prestação de serviços OEV, o modelo CHAPAS, que pretende: (i) desincentivar a comunicação direta entre instituições para a obtenção de informação do cidadão, (ii) colocar o cidadão no controlo da disseminação da sua informação pelas várias instituições e (iii) fomentar a minimização da informação que o cidadão tem de fornecer às várias instituições para obter os serviços que pretende. Para cumprir esses objetivos, transferimos para o cidadão a responsabilidade pela obtenção de todos os serviços que compõem um serviço OEV, e dotámos o cidadão de uma aplicação, o Chappie, que lhe permite: (i) compor o serviço OEV que pretende obter, (ii) verificar que informação tem de fornecer para obter cada um dos serviços que compõem o serviço OEV e, caso o cidadão assim o decida, (iii) proceder à obtenção desses vários serviços. Como o cidadão pode fornecer a cada instituição toda a informação necessária para que esta lhe preste o serviço pretendido, mesmo que tenha de os obter previamente de outras instituições, estas deixam de ter necessidade de comunicar entre si para obter a informação que necessitam para a prestação dos respetivos serviços, o que permite limitar a difusão de informação do cidadão e dessa forma proteger a sua privacidade.

Para a avaliação do modelo usámos o evento da vida de compra de casa, que envolve interações do cidadão com serviços de várias instituições da AP e particulares e cujas características nos permitem explorar as várias vertentes do modelo. Com base nele, desenvolvemos um cenário de exploração e protótipos do Chappie e dos vários serviços, que nos permitiram concluir da viabilidade do modelo CHAPAS, com algumas vantagens e com algumas limitações, para ser uma alternativa viável para a prestação de serviços de governo eletrónico ao cidadão.

keywords

life events, egovernment, egovernment service provision, document agregation, privacy.

abstract

The introduction of Information and Communication Technologies in the Public Administration (PA) gave rise to a huge evolution in the provisioning of public services to the citizen. It evolved from a service provisioning paradigm based in the competences of each PA department, which directly results from the PA siloed organization, into an integrated service provisioning paradigm, that may involve multiple PA departments that exchange information with each other, possibly without the citizen being aware of those exchanges. One of the reasons for this service integration is the provisioning of better services targeted to the satisfaction of citizens' everyday situations that require interaction with many PA services, i.e., life-event services. Despite the goodness in the goal of improving the citizen interaction with PA, the integration of PA services is complex and may create adverse situations for the citizens, namely regarding their privacy. The citizen loses the control over the dissemination of his personal information throughout the many PA departments, as they communicate with each other to gather the information required for service provisioning.

In this thesis, we propose a model for life-event service provision, the CHAPAS model, with the following goals: (i) to discourage direct communication between PA departments to exchange citizens' information; (ii) to place the citizen in control of the dissemination of his information throughout the many PA departments; and (iii) to promote the minimization of the disclosure of citizens' information to PA departments when obtaining the wanted services. To fulfill these goals, we transfer the responsibility for obtaining all the partial services that composes a life event service to the citizen that is empowered with an application, the Chappie, which enables him to: (i) compose the life-event service he wants; (ii) verify the information he must disclose to obtain each and every partial service that composes the life-event service he wants; and upon a citizen decision, (iii) obtain all those partial services. As the citizen is able to supply all the information that a PA department needs to provide the service the citizen wants, departments no longer need to communicate with each other to gather the information they need for service provisioning. This enhances the protection of citizens' privacy as we avoid the dissemination of citizens' information without his control.

For CHAPAS model validation, we used the Buying a Home life event, which requires citizen interactions with services from several PA departments and private institutions, and whose characteristics allows for a full exploration of the model. We developed an exploitation scenario and prototypes for the citizen Chappie and for the several services from which we concluded that the CHAPAS model, with some advantages and some disadvantages, might be a viable alternative for the provisioning of e-government services to citizens.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

ÍNDICE DE EXCERTOS DE CÓDIGO

LISTA DE SIGLAS E ACRÓNIMOS

AP	Administração Pública
CHAPAS	*Citizen-side HAndling of Public Administration e-Services*
Chappie	*Citizen APPlication to Interact with E-services*
CPCV	Contrato Promessa de Compra e Venda
CRP	Conservatória do Registo Predial
e-government	*Electronic Government*
EDS	*Electronic Data Safe*
EIF	*European Interoperability Framework*
ESD	*Electronic Service Delivery*
G2B	*Government to Businesses*
G2C	*Government to Citizen*
G2G	*Government to Government*
GovML	*Government Markup Language*
IdP	*Identity Provider*
IPS	Instituição Prestadora de Serviços
NIC	Número de identificação Civil (antigo número do Bilhete de Identidade)
NIF	Número de Identificação Fiscal
NISS	Número de Identificação da Segurança Social
NPM	*New Public Management*
PCC	Processo de Compra de Casa
PDE	*Personal Data Ecosystem*
Portal OEV	Portal Orientado a Eventos da Vida
RDP	*Required Documents Policy* (Política de Documentos Necessários)
RP	*Relying Party*
Serviço OEV	Serviço Orientado a Eventos da Vida
SSO	*Single Sign-On*
TIC	Tecnologias da Informação e Comunicação

1 INTRODUÇÃO

A Administração Pública (AP) tem sofrido nas últimas décadas um grande conjunto de transformações, em parte desencadeadas pela introdução das Tecnologias da Informação e da Comunicação (TIC). Estas transformações são particularmente evidentes na forma como a prestação de serviços da AP aos seus clientes, cidadãos e empresas, evoluiu. Transitou-se de um modelo de organização da AP com organismos com um elevado grau de independência e pouco comunicantes, designada organização em silos, com um paradigma de prestação de serviços discretos focados nas competências dos respetivos organismos, para um modelo de organização do estado em que todos os organismos da AP estão interligados entre si, o designado *whole-of-government* (T. Christensen & Laegreid 2007), com um paradigma de prestação de serviços eletrónicos transversais aos diversos organismos, focados na eficiência da AP e nas necessidades e interesses dos clientes da AP.

Um dos modelos de prestação de serviços transversais ao cidadão é a designada *prestação de serviços orientados a eventos da vida* (serviços OEV) (Wimmer & Tambouris 2002; Vintar et al. 2002), i.e., serviços alinhados com as necessidades que os cidadãos sentem no seu dia-a-dia e para cuja satisfação necessitam de interagir com serviços da AP. Normalmente integram vários serviços, tipicamente prestados por diferentes organismos, de forma que o cidadão não tenha necessidade de interagir individualmente com cada um desses organismos e, no limite, nem tenha a perceção da participação desses múltiplos organismos na prestação do serviço. Obviamente, devido à simplificação que estes serviços criam na interação do cidadão com a AP, eles têm um grande potencial de aceitação por parte da comunidade, o que cria expetativas e pressões para a extensão do modelo à generalidade da AP, o que pode levar a que possa, eventualmente, haver alguma subavaliação das características destes serviços que acarretem aspetos menos positivos, como é o caso da privacidade dos cidadãos.

1.1 MOTIVAÇÃO

Um dos principais problemas do paradigma da prestação de serviços discretos é a dificuldade na interação do cidadão com os organismos da AP. Com efeito, é frequente o cidadão ter de interagir com vários organismos da AP para resolver uma sua necessidade, como a aquisição ou construção de uma casa, por exemplo. O cidadão tem de se deslocar, física ou virtualmente, a um organismo para obter um determinado documento que depois tem de entregar noutro organismo, eventualmente em conjunto com documentos obtidos ainda noutros organismos, e isto sucessivamente até que finalmente consiga satisfazer a sua necessidade. Esta forma de relacionamento com o cidadão tem neste óbvios impactos negativos, o que provoca o seu descontentamento e desmotivação para interagir com a AP.

No entanto, devido ao não-fomento da comunicação direta entre organismos da AP, o paradigma da prestação de serviços discretos apresenta duas características que, do ponto de vista da privacidade do cidadão, podem ser vistas como vantagens. A primeira característica é que cada organismo fica com posse exclusiva da informação prestada pelo cidadão, o que cria obstáculos ao cruzamento desses dados e, por consequência, à construção de perfis únicos dos cidadãos com base na totalidade da informação que o Estado (nos seus vários organismos) possui sobre eles. Note-se que o estado é detentor de informação privilegiada sobre os cidadãos, sendo muita desta obtida de forma compulsiva. A segunda característica é que o cidadão tem um papel ativo na disseminação da sua informação pelos vários organismos (através da entrega de documentos que tem de ir obter noutros organismos), o que lhe permite, por um lado, estar ciente de qual a informação que cada organismo possui sobre si e, por outro, dentro de alguns limites, ter algum controlo e poder de oposição relativamente ao fornecimento de informação que considere excessiva.

A progressiva introdução das TIC na AP, a sua progressiva sofisticação e as transformações que desencadearam, vieram possibilitar novas abordagens à prestação de serviços da AP ao cidadão. Invariavelmente, estas abordagens preconizam a comunicação entre organismos, seja apenas para colaboração ou mesmo para a sua integração, implementada através da partilha de dados ou através da participação em processos transversais (Klischewski 2004), justificando-a com reduções de custos para todos os intervenientes, AP e cidadãos, e em melhores e mais cómodos serviços para o cidadão, de que é corolário a prestação de serviços orientados a eventos da vida (serviços OEV) (Vintar et al. 2002; Wimmer & Tambouris 2002). No entanto, sendo claro que toda esta interação entre organismos traz grandes benefícios para a AP (e indiretamente para todos

nós que para ela contribuímos) – uma maior eficácia e redução de custos – e para os cidadãos – uma maior comodidade e menores custos de acesso aos serviços –, ela trouxe também novos desafios e dificuldades. Para a AP, porque é necessário garantir a interoperabilidade entre organismos, o que não é fácil e tem implicações a vários níveis (Lam 2005; Eynon 2007; Hellman 2010). Para os cidadãos, porque não é claro que a proteção da sua privacidade tenha saído beneficiada (Bannister 2005).

1.2 PROBLEMA

A interligação dos diversos organismos da AP potencia um maior fluxo de dados entre organismos, o que traz como benefício a possibilidade de prestação de serviços mais eficientes, mais eficazes e mais adequados às necessidades dos cidadãos, como é o caso dos serviços OEV. No entanto, esse maior fluxo de dados traz também associado o risco da eventual utilização desses mesmos dados para outros fins que não os anunciados e eventualmente sem o conhecimento e sem o controlo dos cidadãos (Belanger & Hiller 2006). Por exemplo, podem ser cruzados e agregados para a criação de perfis únicos dos cidadãos, englobando várias vertentes do contacto do cidadão com a AP, como a saúde, finanças, justiça, educação, etc. Dado o caracter confidencial e obrigatório de muita da informação na posse dos organismos da AP, esta possibilidade de cruzamento de dados tem o potencial de poder agravar, em favor do Estado, as naturais assimetrias de poder entre o Estado e o cidadão, com todas as consequências que daí podem advir, inclusive para a própria subsistência da democracia (Nissenbaum 2004).

É claro que podem ser tomadas medidas que combatam e minimizem o problema mas, por um lado, serão sempre internas à própria AP, isto é, fora do controlo do cidadão, e, por outro, podem levar a um aumento substancial da complexidade e, consequentemente, dos custos dos sistemas que permitem a integração e a interoperabilidade.

1.3 OBJETIVOS

O objetivo deste trabalho é propor um modelo de prestação de serviços que concilie as vantagens do paradigma de prestação de serviços discretos com as vantagens do paradigma de prestação de serviços transversais. Ou seja, um modelo que permita a

prestação de serviços eletrónicos orientados aos interesses do cidadão, serviços OEV, envolvendo a participação de vários organismos, que mantenha o cidadão efetivamente no controlo da execução do serviço e do fluxo de informação entre organismos necessário para a prestação dos serviços pretendidos, e que possibilite a minimização desta informação fornecida pelo cidadão ao mínimo indispensável para permitir a prestação do serviço pretendido pelo cidadão.

1.4 CONTRIBUIÇÃO

A contribuição principal deste trabalho é a proposta de um modelo de prestação de serviços OEV, o modelo CHAPAS (*Citizen-side HAndling of Public Administration e-Services*). Neste modelo, o cidadão, auxiliado por uma aplicação pessoal, o Chappie (*Citizen APPlication to Interact with E-services*), compõe o serviço OEV pretendido (i.e., define o conjunto de serviços parciais que deve ser obtido das várias instituições), de acordo com um modelo em árvore de dependências, e controla a obtenção dos vários serviços parciais.

Ao transferir para o cidadão a responsabilidade da obtenção dos vários serviços parciais, colocámo-lo no controlo do fluxo de informação entre instituições que é necessário para a prestação dos vários serviços, o que lhe permite verificar e ficar com o conhecimento de que informação divulga a cada instituição, quando e por que razão. Por outro lado, como o cidadão fornece toda a informação que uma instituição necessita para que preste um serviço por ele pretendido, ainda que a tenha de ir obter a outras instituições, evita-se que as instituições comuniquem entre si para obter informação sobre o cidadão. Adicionalmente, o modelo CHAPAS fornece mecanismos que permitem a minimização da informação fornecida pelo cidadão a cada instituição ao mínimo estritamente necessário para a prestação dos serviços, no qual se inclui um mecanismo que permite a agregação de documentos com base em atributos ofuscados, ou seja, sem revelar a identidade do cidadão (ou outras entidades) a que os documentos se referem. Este último mecanismo é igualmente uma contribuição importante deste trabalho, consubstanciada numa patente.

Foi também desenvolvido um cenário de exploração, com base no evento da vida compra de casa, e um protótipo com base em tecnologia Web Services, para avaliar (i) a viabilidade da modelação de serviços OEV como árvores de dependências; (ii) a exequibilidade de um motor para a construção de árvores de dependências e a

subsequente obtenção dos serviços que a compõem; e ainda (iii) a viabilidade da agregação de documentos com base em atributos ofuscados.

1.5 PUBLICAÇÕES E OUTRAS AÇÕES DE DISSEMINAÇÃO DA INVESTIGAÇÃO REALIZADA

Ao longo do doutoramento de que resultou esta tese publicámos diversos artigos em atas de conferências e obtivemos uma patente nacional.

Os artigos publicados em atas de conferências que estão fortemente relacionados com o conteúdo desta tese são os seguintes:

[1] Artigo (*position paper*) onde fazemos a apresentação da ideia do modelo CHAPAS e fazemos a discussão de algumas das suas características, pontos fortes e pontos fracos.

Hélder Gomes, André Zúquete, and Gonçalo Paiva Dias, "Citizen-Side Handling of Life Event Services," *WEBIST 2012 - 8th International Conference on Web Information Systems and Technologies*, Porto - Portugal, pp. 565–570, 2012.

[2] Artigo onde apresentamos a prestação de serviços OEV no modelo CHAPAS e introduzimos os conceitos de Política de Documentos Necessários (RDP – *Required Documents Policy*) e de modelação de serviços em árvore de dependências construídas com base nas RDP dos múltiplos serviços envolvidos num serviço OEV.

Hélder Gomes, André Zúquete, and Gonçalo Paiva Dias, "Citizen Controlled Exchange of Information in E-government", WEBIST 2011 - 7th International Conference on Web Information Systems and Technologies, Noordwijkerhout, The Netherlands, pp. 494–499, 2011.

A patente que obtivemos, também fortemente relacionada com o trabalho desta tese, é a seguinte:

[3] Patente sobre o processo de agregação de informação com base em atributos com os seus valores ofuscados utilizando parâmetros de ofuscação definidos pelo utente. Este processo permite que uma instituição possa agregar

documentos fornecidos por um utente sem que para isso tenha acesso aos valores originais dos atributos usados para a agregação.

Hélder Gomes, André Zúquete, e Gonçalo Paiva Dias. PROCESSO DE AGREGAÇÃO DE ATRIBUTOS DE UM UTENTE COM GARANTIA DE PRIVACIDADE. Patente PT-105979. Início de vigência: 31-10-2011.

No âmbito do trabalho de investigação desenvolvido durante o doutoramento foram também investigados tópicos relacionados com o assunto central desta tese, o modelo CHAPAS, nomeadamente: (i) a exploração de dispositivos pessoais para autenticação eletrónica de cidadãos, (ii) a privacidade dos cidadãos face a serviços prestados pela AP e (iii) aspetos gerais relativos à implantação de serviços de governo eletrónico. Desse trabalho resultaram várias publicações que não têm uma contribuição direta para o assunto central desta tese, mas que de certa forma inspiraram algumas das decisões tomadas ao longo da mesma.

Os dispositivos pessoais para autenticação eletrónica, vulgarmente designados por dispositivos (*tokens*) eID, têm vindo a ser adotados em inúmeros países, como por exemplo em Portugal, onde o Cartão de Cidadão tem vindo a ser introduzido gradualmente desde 2007. Sendo a autenticação dos cidadãos um requisito incontornável de qualquer sistema real criado com base no paradigma CHAPAS, desde cedo ficou claro que a mesma poderia usufruir do facto dos cidadãos disporem de um eID que os pudesse identificar perante os serviços. Nesse sentido, foram realizadas várias iniciativas de investigação envolvendo o eID Português, das quais resultaram duas publicações em atas de conferências:

[4] Artigo onde apresentamos uma aplicação que permite a um utilizador partilhar ficheiros de forma segura através de plataformas de partilha de ficheiros (e.g., DropBox). Nomeadamente, esta aplicação permite a autenticação dos utilizadores através da utilização do Cartão de Cidadão.

Eduardo Duarte, Filipe Pinheiro, André Zúquete, and Hélder Gomes, “Secure and Trustworthy File Sharing Over Cloud Storage Using eID Tokens”, in Open Identity Summit 2014, Lecture Notes in Informatics, vol. P-237, D. Hühnlein and H. Roßnagel, Eds. Gesellschaft für Informatik, 2014, pp. 73–84.

[5] Artigo onde apresentamos o conceito de *Personal Identity Provider* (PIdP) que permite a autenticação de utilizadores em sessões Web usando o seu Cartão

de Cidadão, e a sua integração na infraestrutura de autenticação baseada em Shibboleth[1] da Universidade de Aveiro.

André Zúquete, Hélder Gomes, Cláudio Teixeira, "Personal Identification in the Web Using Electronic Identity Cards and a Personal Identity Provider", in Lecture Notes in Computer Science, vol. 8051, D. Naccache and D. Sauveron, Eds. Springer Berlin Heidelberg, 2014, pp. 160–169.

Porém, o tema da autenticação não foi suficientemente aprofundado no âmbito do doutoramento, não se tendo chegado ao ponto de efetivamente explorar o Cartão de Cidadão na prova de conceito apresentada no Capítulo 4. De qualquer modo, nesse capítulo é dada uma perspetiva de alto nível de como o mesmo poderia ser explorado seguindo a aproximação arquitetural descrita no artigo acima referido.

Relativamente à privacidade dos cidadãos na sua relação com a AP, fez-se um estudo empírico da qualidade dos serviços prestados ao cidadão relativamente à preservação da sua privacidade, do qual resultou a seguinte publicação:

[6] Gonçalo Paiva Dias, Hélder Gomes, André Zúquete, "Privacy Policies in Web Sites of Portuguese Municipalities: An Empirical Study", in *Advances in Information Systems and Technologies*, vol. 206, Á. Rocha, A. M. Correia, T. Wilson, and K. A. Stroetmann, Eds. Springer Berlin Heidelberg, 2013, pp. 87–96.

Relativamente à implantação de serviços de governo eletrónico temos um artigo publicado e outro aceite para publicação:

[7] Gustavo Gouvêa Maciel, Hélder Gomes, Gonçalo Paiva Dias. "Evaluating Local E-government Maturity in Selected Iberoamerican Countries", *10th Iberian Conference on Information Systems and Technologies (CISTI),* Águeda, Portugal, 2015 (aceite)

[1] http://shibboleth.net

[8] Gonçalo Paiva Dias, Hélder Gomes, "Evolution of local e-government maturity in Portugal", *9th Iberian Conference on Information Systems and Technologies (CISTI),* Barcelona, Espanha, pp. 395-399, 2014.

Ainda no contexto do doutoramento publicámos um último artigo cujo conteúdo não tem relação direta com o assunto desta tese. A ideia original do trabalho de tese era a utilização de ontologias para harmonização de sistemas de controlo de acesso entre organizações que tivessem de colaborar, pelo que foi feito um estudo sobre a utilização de ontologias na área da segurança informática do qual resultou o seguinte artigo:

[9] Hélder Gomes, André Zúquete, Gonçalo Paiva Dias. "An Overview of Security Ontologies." *9ª Conferência da Associação Portuguesa de Sistemas de Informação (CAPSI 2009)*, Viseu, Portugal, Outubro 2009.

Por fim, importa referir que, no âmbito da disseminação da investigação feita durante o doutoramento, o conceito central desta dissertação, o modelo CHAPAS, foi a base do projeto de investigação EVOL (Events Of Life - Making Citizen´s Life Easier), que foi objeto em 2014 de uma candidatura a financiamento pelo programa europeu Horizonte2020, proposto por um consórcio de empresas liderado pela empresa espanhola ATOS SPAIN SA, e no qual participavam duas universidades, a Universidade de Aveiro e austríaca Graz University of Technology, duas empresas portuguesas, a ICTECH (Information & Communication Technologies, Lda) e a Shortcut, um consórcio de entidades públicas italianas, a CSI-Piemonte, uma empresa austríaca sem fins lucrativos e também um centro de competência em segurança, o Austria Secure Information Technology Center, e uma outra empresa espanhola, a Firmaprofesional, SA. No entanto, a candidatura não obteve aprovação, para o que contribuiu o grau de rotura do CHAPAS relativamente ao status quo, fortemente orientado para a integração de serviços do lado dos prestadores de serviços.

1.6 ORGANIZAÇÃO

Este documento está organizado em cinco capítulos e um anexo. Começa com este primeiro capítulo no qual se indica a motivação, se descreve o problema, se

apresentam os objetivos e a contribuição deste trabalho, se indicam as publicações e a estrutura do documento.

No segundo capítulo faz-se uma contextualização do trabalho e apresenta-se o trabalho relacionado. Começamos por apresentar uma panorâmica da evolução da prestação de serviços eletrónicos da AP, na secção 2.1, após o que apresentamos alguns conceitos relevantes sobre a identificação dos cidadãos, na secção 2.2. De seguida, na secção 2.3, apresentamos o conceito de arquitetura SOA e de *Web Services*, nos quais se baseia o modelo desenvolvido neste trabalho. Finalmente, na secção 2.4, apresentamos um conjunto de abordagens que têm como objetivo reforçar o controlo do cidadão sobre os seus dados pessoais ou sobre a obtenção de serviços, transferindo funcionalidades para o seu lado. Concluímos, na secção 2.5, com um resumo da informação apresentada no capítulo.

No terceiro capítulo apresentamos o modelo CHAPAS para a prestação ao cidadão de serviços OEV. Começamos por apresentar os objetivos do modelo. Depois apresentamos, na secção 3.2, o modelo de prestação de serviços orientados a eventos da vida, ao que se segue, na secção 3.3, a apresentação da forma como estes serviços são compostos e como se processa a sua obtenção e, na secção 3.4, a apresentação dos vários padrões de interação do Chappie com as instituições prestadoras de serviços com vista à obtenção dos serviços por elas prestados. Na secção 3.5 apresenta-se o conceito de documento, o veículo de comunicação de informação entre instituições, e de atributo, o elemento básico de informação dentro de cada documento. Na secção 3.6 apresenta-se a forma como o modelo CHAPAS fomenta a minimização da informação a fornecer pelo cidadão e, na secção 3.7, apresenta-se o mecanismo para a agregação de documentos com base em atributos ofuscados, que permite realizar a agregação de documentos sem revelar certos atributos de identidade das entidades a que os documentos se referem. Depois, na secção 3.8, apresentamos a RDP (*Required Documents Policy*), um documento que especifica os requisitos que uma instituição coloca para a obtenção de um determinado serviço, que é uma peça fundamental para permitir a prestação de serviços no modelo CHAPAS. De seguida, na secção 3.9, fazemos a discussão de um conjunto de aspetos relevantes do modelo CHAPAS, após o que apresentamos as conclusões, na secção 3.10.

No quarto capítulo fazemos a prova de conceito do modelo CHAPAS. Começamos por apresentar, na secção 4.1, o evento da vida selecionado para a prova de conceito: a compra de casa por um cidadão. Depois, na secção 4.2, apresentamos o cenário de exploração desenvolvido para o evento de vida selecionado. Na secção 4.3 apresentamos o

protótipo desenvolvido e, na secção 4.4, apresentamos a exploração do cenário usando o protótipo. Na secção 4.5 fazemos a discussão e validação da prova de conceito e concluímos, na secção 4.6 com um resumo do capítulo.

No quinto capítulo concluímos, fazendo algumas considerações acerca das contribuições deste trabalho e sobre o trabalho futuro.

2 CONTEXTUALIZAÇÃO E TRABALHO RELACIONADO

Neste capítulo vamos apresentar e discutir alguns assuntos relevantes para a contextualização deste trabalho. Começamos por apresentar, na secção 2.1, uma panorâmica da evolução da prestação de serviços de governo eletrónico ao cidadão, com particular enfoque na prestação de serviços orientados a eventos da vida. Na secção 2.2, apresentamos alguns conceitos sobre identificação, fundamentais para perceber alguns dos aspetos do modelo CHAPAS.

Na secção 2.3 fazemos uma breve apresentação da arquitetura SOA, o paradigma de desenvolvimento de aplicações distribuídas que se baseia na combinação e reutilização de serviços como componentes. Na secção 2.3 analisamos aplicações centradas no utilizador com potencial para ser usadas na prestação de serviços de governo eletrónico. Por fim, na seção 2.5, terminamos com um resumo dos conceitos apresentados.

2.1 PRESTAÇÃO DE SERVIÇOS DE GOVERNO ELETRÓNICO

Nesta secção apresentamos uma panorâmica da evolução da prestação dos serviços de governo eletrónico, com particular enfoque nos aspetos relevantes para este trabalho. Começamos por fazer uma apresentação do conceito de governo eletrónico, na secção 2.1.1, da evolução do governo eletrónico, na secção 2.1.2. Na secção 2.1.3 apresentamos o conceito de prestação de serviços discretos e, na secção 2.1.4, o conceito de prestação de serviços integrados centrados no cidadão. De seguida, na secção 2.1.5, apresentamos o paradigma de prestação de serviços OEV, após o que, na secção 2.1.6,

analisaremos alguns aspetos de interoperabilidade, condição indispensável para que possa haver prestação de serviços integrados, e concluímos na secção 2.1.7 com algumas reflexões sobre a confiança dos cidadãos na prestação de serviços do Estado.

2.1.1 CONCEITO DE GOVERNO ELETRÓNICO

O governo eletrónico (*e-government*), com maior ou menor expressão, é hoje uma realidade em praticamente todos os países do mundo, como podemos constatar nos relatórios das Nações Unidas de avaliação do governo eletrónico (United Nations 2008; United Nations 2010; United Nations 2012; United Nations 2014). Não existe, no entanto, uma unanimidade quanto ao conceito de governo eletrónico (Relyea 2002; Yildiz 2007). Assim, encontramos definições, que o limitam à divulgação de informação e à prestação de serviços aos cidadãos e empresas (Jeff 2000; Silcock 2001; United Nations & American Society for Public Administration 2002), outras mais latas que também incluem as políticas públicas e os processos democráticos (European Commission 2003b) e outras ainda que o consideram como um processo contínuo de reorganização da AP (Baum et al. 2000; Fountain 2001). Apesar das diferenças de âmbito e de impacto nestas definições, existe um denominador comum entre elas: a utilização das TIC, com especial relevância para a Internet, para uma melhor prestação de serviços do governo aos seus clientes – cidadãos, empresas e outros organismos do governo (Palvia & Sharma 2007), implicando a reinvenção do sector público através da transformação das formas de fazer as coisas e dos relacionamentos com cidadãos e empresa (Ndou 2004). É esta visão de governo eletrónico orientada à prestação de serviços eletrónicos aos cidadãos, *e-services* (Löfstedt 2005; Nordfors et al. 2009), aquela que melhor se adequa ao contexto deste trabalho.

É importante uma nota prévia em relação ao termo governo eletrónico. Este termo generalizou-se em português com um sentido que não se restringe ao governo, enquanto órgão executivo (utilização correta do termo governo em português), mas com um sentido mais lato que se aplica a toda a AP e a outros órgãos de administração e até a instituições privadas que prestam serviços de utilidade pública. Esta aplicação é semelhante à do termo inglês *electronic government*, do qual deriva, e do qual herdou o sentido (Dias 2006). É com este sentido mais lato que empregamos o termo.

A prestação de serviços eletrónicos (*ESD* - *Electronic Service Delivery*) pode ser feita através de diversos canais eletrónicos como, por exemplo, o telefone, quiosques ou a Internet. No contexto deste trabalho vamo-nos focar na prestação de serviços de governo

eletrónico através da Internet, que podem ser prestados por instituições públicas (organismos da AP, entidades Municipais, etc.) ou privadas (bancos, companhias de seguros, notários, etc.), que genericamente designaremos como instituições.

As iniciativas de governo eletrónico têm sido classificadas em função das entidades a que se destinam os serviços disponibilizados, nomeadamente cidadãos, empresas, funcionários da AP e outras entidades da AP, através das siglas G2C (*Government to Citizen*), G2B (*Government to Business*es), G2E (*Government to Employees*) e G2G (*Government to Government*), respetivamente (Ndou 2004). De acordo com esta classificação, este trabalho enquadra-se maioritariamente na perspetiva de G2C, uma vez que se foca essencialmente em aspetos relacionados com a prestação de serviços eletrónicos ao cidadão. No entanto, aspetos de G2G são utilizados como justificação para a pertinência da abordagem à prestação de serviços ao cidadão que propomos.

Em relação à prestação de serviços G2C, a sua lógica deve ser a de servir os interesses do cidadão, i.e., estarem centrados no cidadão (*citizen-centric*), por oposição ao interesse das instituições que os prestam (United Nations 2010).

2.1.2 EVOLUÇÃO DA PRESTAÇÃO DE SERVIÇOS DE GOVERNO ELETRÓNICO AO CIDADÃO

O conceito de prestação de serviços centrados no cidadão (*citizen-centric*) tem as suas raízes no movimento conhecido por *New Public Management* (NPM) (Schedler & Proeller 2000), que preconizava a prestação de serviços competitivos e eficientes. Surgiu como reação à burocracia weberiana (Church & Moloney 2012), cara, burocrática e com uma AP organizada em instituições com lógicas funcionais e rígidas, i.e., uma organização em silos (De Bri & Bannister 2010).

O NPM colocou o cidadão no centro da missão da AP, através de medidas de flexibilização da gestão inspiradas no mundo empresarial e a incorporação de lógicas de competição e mercado (United Nations 2008). Isto deu origem a um movimento de descentralização e fragmentação, com a criação de novas agências autónomas especializadas em assuntos específicos (nichos), por vezes ao seu *outsourcing*, e ao fomento da competição entre agências com o objetivo de reduzir custos e prestar serviços de melhor qualidade, mas que no fundo gerou ainda mais silos (Howard 2014).

Esta autonomia entre instituições da AP, deu origem a uma primeira geração de iniciativas de governo eletrónico, conduzidas individualmente por cada instituição (organismo da AP, poder local, empresa pública, etc.) com o objetivo de transportar para a Internet os serviços por eles prestados ao público (United Nations 2008). É um modelo de prestação de serviços disperso, no sentido que não há qualquer colaboração entre instituições para a prestação de serviços (Vintar et al. 2002; Dias 2011). Os serviços que cada instituição presta são função exclusivamente das suas competências, pelo que este modelo também se designa como um modelo centrado-no-governo (*government-centric*) (United Nations 2010).

Numa segunda geração de iniciativas de governo eletrónico, o enfoque foi colocado no conceito de *whole-of-government* (T. Christensen & Laegreid 2007), ou de *joining-up government* (Bellamy 1999), i.e., numa AP em que as várias instituições comunicam, colaboram e se coordenam para alcançar objetivos partilhados e respostas integradas (United Nations 2008). Pretende-se com isso a redução de custos de operação e a prestação de melhores serviços ao cidadão. Trata-se de um modelo de prestação de serviços integrados, i.e. em que várias instituições colaboram para a prestação de um serviço do interesse do cidadão, pelo que também se designa como centrado no cidadão (*citizen-centric*) (United Nations 2010).

2.1.3 PRESTAÇÃO DE SERVIÇOS DISPERSA

A prestação de serviços ao cidadão é considerada dispersa quando os serviços prestados pelas instituições são definidos de acordo com as atribuições e os interesses da respetiva instituição, não havendo preocupações com a integração de serviços para melhor servir o cidadão (Vintar et al. 2002; Dias 2011). Esta é a aproximação tradicional. Este modelo de organização da AP tem um grande impacto no cidadão por normalmente ser necessária a participação de várias instituições (dos seus serviços) para a resolução/satisfação de situações concretas do dia-a-dia do cidadão, o que tem dois tipos de implicações: por um lado, ao nível da complexidade da interação do cidadão com a AP (Dias & Rafael 2007) e por outro ao nível dos custos que acarreta para o cidadão (Dias & Narciso 2010).

O envolvimento/participação de serviços de várias instituições na solução de uma necessidade do cidadão implica uma determinada sequência na obtenção destes

serviços. Tipicamente, o resultado de um serviço alimenta um serviço que se segue numa cadeia de serviços, ou *workflow* (Hollingsworth 1995), que no final resulta na satisfação da situação do cidadão. Esta cadeia de serviços, mais ou menos complexa, é gerida pelo cidadão e é claramente um obstáculo no acesso dos cidadãos à AP, porque implica que os cidadãos conheçam a organização da AP e as competências dos vários organismos, para que possam determinar o conjunto de serviços que precisam obter para satisfazer as suas necessidades concretas (Dias & Rafael 2007).

Do ponto de vista dos custos para o cidadão, ela obriga o cidadão a deslocar-se aos balcões, físicos ou virtuais, das várias instituições que prestam os serviços que o cidadão necessita. No caso da interação com balcões físicos, implica, pelo menos, elevados custos ao nível do tempo necessário para a obtenção dos vários serviços e ao nível do transporte do cidadão entre os balcões das várias instituições. No caso da interação em balcões virtuais, implica também custos ao nível do tempo devido à necessidade de conciliação dos vários serviços. Note-se que a análise do tempo para a obtenção de um serviço pode ser vista sob a perspetiva do tempo gasto nas interações com o balcão e na perspetiva do tempo que a instituição demora a prestar o serviço, após a realização do seu pedido. Para o nosso trabalho, a perspetiva mais relevante é a primeira.

Do ponto de vista da privacidade, este modelo traz claros benefícios para o cidadão, uma vez que os seus dados se encontram fracionados pelas várias instituições (Bannister 2005). Não havendo comunicação entre estas, ou não havendo a integração dos dados à guarda de cada uma delas, existe um claro obstáculo à exploração global desses dados para, por exemplo, construir perfis dos cidadãos. Além disso, como é o cidadão que controla a execução da cadeia de serviços, nos casos em que existam várias instituições a prestar um mesmo serviço de forma concorrente, ele tem o poder de escolher qual a instituição onde vai obter o serviço. Por outro lado, como o cidadão controla o fluxo de dados, transportando os resultados de um serviço para o serviço seguinte na cadeia, ele pode verificar que dados fluem entre organismos, o que lhe permite a tomada de ações/atitudes caso entenda que algum serviço pretende obter dados cuja necessidade ele não perceba ou com a qual ele não concorde.

Porém, e ainda relacionado com a privacidade do cidadão, há um aspeto neste modelo que é uma desvantagem para o cidadão. Com o objetivo de sistematizar os seus processos internos, os documentos que as instituições emitem possuem normalmente um formato padrão, cujo conteúdo está adaptado para fornecer informação para o maior número possível de instituições que poderão vir a receber o documento. Como não é

líquido que todas as instituições que potencialmente possam vir a receber um desses documentos precisem da totalidade da informação lá contida, existe a possibilidade de haver instituições a receber mais informação do que a estritamente necessária para a prestação do serviço pretendido.

2.1.4 PRESTAÇÃO DE SERVIÇOS INTEGRADOS

Como reação à excessiva fragmentação da AP, surgem os conceitos de *joined-up government* (Bellamy, 1999) e *whole-of-government* (T. Christensen & Laegreid 2007). Ambos os conceitos preconizam uma AP integrada e coerente onde os vários organismos partilham objetivos e colaboram com vista a produzir uma resposta integrada (United Nations 2008), i.e., prestam serviços integrados. Pretendem, assim, promover a redução de custos e prestar serviços de melhor qualidade e mais valor aos cidadãos e a outros clientes (United Nations 2008).

A "integração em governo eletrónico é a formação de uma unidade de instituições do Estado, temporárias ou permanentes, tendo como objetivo a fusão de processos e/ou a partilha de informação" (Scholl & Klischewski 2007). Serviços integrados são pois serviços que integram recursos de diversas instituições, sendo as estratégias para o seu desenvolvimento baseadas na partilha de dados ou na integração de processos (Klischewski 2004). A primeira destas estratégias é comum nos Estados Unidos, enquanto a segunda o é na Europa. Assim, mais num contexto europeu, um serviço integrado é definido como um serviço que integra dentro de si vários outros serviços, eventualmente de múltiplas instituições, mas que se apresenta com sendo um serviço único (Cukjati & Todorovski 2008). Esta integração de serviços é interessante porque raramente as situações que os cidadãos enfrentam no seu dia-a-dia, e que exigem serviços da AP, são satisfeitas com a obtenção de um único serviço, mas quase sempre com a obtenção de um conjunto de serviços, cada um deles prestado por uma instituição diferente. É esta a vertente de integração que exploramos neste trabalho.

A satisfação de uma necessidade dos cidadãos normalmente envolve a obtenção de não apenas um serviço, mas sim de um conjunto de serviços prestados por diferentes instituições, o que normalmente acarreta dificuldades e custos acrescidos. Por prestação de serviços centrados no cidadão entende-se a prestação de serviços que satisfaçam necessidades efetivas dos cidadãos, quaisquer que sejam as instituições envolvidas na sua prestação, por oposição à prestação de serviços centrados nas instituições, sendo

suportados pela integração e consolidação de serviços, processos e sistemas das várias instituições. É no sentido integrar a prestação de um conjunto de serviços, de modo a adequá-los aos interesses dos cidadãos, que se enquadram os balcões únicos (*one-stop shops*) (Kubicek & Hagen 2000; Wimmer & Tambouris 2002; Trochidis et al. 2008) e a prestação de serviços OEV (Wimmer & Tambouris 2002; Vintar et al. 2002).

Os balcões únicos são locais onde o cidadão pode aceder aos vários serviços da AP sem ter que se preocupar em saber quais as instituições da AP que efetivamente os prestam. Trata-se da integração do *front office* dos vários organismos num único *front office*, de forma que os serviços destes organismos possam ser prestados num balcão comum. Por *front office* entende-se o ponto de contacto com o cidadão, por oposição ao *back office* que corresponde à retaguarda, não visível pelo cidadão, onde é realizado muito do processamento necessário para a prestação do serviço (Cukjati & Todorovski 2008). Evitam-se assim os incómodos e inconvenientes das deslocações entre instituições que são característicos da prestação de serviços dispersa. Na vertente de prestação de serviços através do canal Internet, os balcões únicos são implementados em portais únicos (*one-stop portals*), frequentemente orientados a públicos-alvo, como é o caso, em Portugal, do Portal do Cidadão[2] e do Portal da Empresa[3].

A prestação de serviços OEV é o principal enfoque desta tese, pelo que será abordada especificamente na secção seguinte.

Para que a prestação de serviços integrados seja possível, há um requisito incontornável: a interoperabilidade (European Commission 2003a; Gottschalk 2009) entre os vários organismos. Isto é, a capacidade de comunicar e de colaborar com vista a atingir um objetivo comum. Este assunto será abordado na secção 2.1.6.

2.1.5 SERVIÇOS ORIENTADOS A EVENTOS DA VIDA (OEV)

Não existe uma definição consensual do conceito de eventos da vida. Por um lado, "*Eventos da vida descrevem situações dos seres humanos que podem necessitar de serviços públicos*"[4] (Wimmer & Tambouris 2002) ou "*eventos da vida são uma metáfora usada para*

[2] http://www.portaldecidadao.pt
[3] http://www.portaldaempresa.pt
[4] "Life-events describe situations of human beings where public services may be required."

situações do dia-a-dia dos cidadãos que exigem a obtenção de um conjunto de serviços públicos"[5] (Todorovski et al. 2006). Nestas definições o enfoque é colocado nas situações das pessoas que podem gerar a necessidade de serviços públicos. Exemplos destas situações do dia-a-dia são: o nascimento de um filho, o ser vítima de um crime, a compra de uma casa, etc.

Por oposição, numa outra definição, o "*termo eventos da vida refere-se aos serviços do governo necessários em momentos específicos da vida* …"[6] (European Commission 2003b). Ainda numa outra definição, mais técnica e detalhada, "*um evento da vida é um conjunto de ações personalizado, incluindo pelo menos um serviço público, que, quando executado num workflow apropriado, satisfaz uma necessidade do cidadão resultante de uma situação da sua vida*"[7] (Momotko et al. 2006). Estas últimas definições colocam o enfoque nos serviços públicos que são necessários para satisfazer uma necessidade do dia-a-dia dos cidadãos.

Para evitar esta variação de enfoque existente em relação à expressão evento da vida, ela será usada quando pretendermos referir uma situação do dia-a-dia dos cidadãos que pode necessitar de serviços públicos e utilizaremos a expressão serviço orientado a eventos da vida (serviço OEV) para nos referirmos a um serviço integrado, que pode envolver serviços públicos de várias instituições, e cujo objetivo é dar resposta a um evento da vida dos cidadãos.

No contexto do projeto europeu OneStopGov foi desenvolvida a ontologia de eventos da vida (*life-event ontology*) que sistematiza o conceito de serviço OEV (Trochidis et al. 2007). Nela, um serviço OEV destina-se a um cidadão e consiste num ou mais serviços públicos. Um serviço público tem como entrada documentos, que podem ser documentos oficiais da AP, produzidos por outros serviços da AP (e.g. certificado de nascimento) ou documentos genéricos não produzidos pela AP (e.g. uma fotografia). Como saída, um serviço público produz sempre um documento oficial da AP. Por outro lado, um serviço público é governado por um conjunto de regras, definidas em leis e regulamentos, que definem os documentos de entrada e saída, bem como a lógica de funcionamento

[5] "Life event is a metaphor used to denote specific situation or event in the life of a citizen that requires a set of public services to be performed."

[6] "*The term 'life events' refers to the government services needed at specific stages in life, …*"

[7] "*… a life-event is a profile-based (personalised) set of actions, including at least one public service, which, when executed in its appropriate workflow, fulfils a need of a citizen arising from a new life situation.*"

interno. Estas regras têm em consideração o perfil ou as circunstâncias do cidadão para determinar a elegibilidade deste para a obtenção do serviço ou para a determinação dos documentos de entrada em concreto que devem ser fornecidos. Por exemplo, para se poder casar (obter o serviço de casamento) um cidadão com 16 ou 17 anos de idade (menor de idade) têm de apresentar uma autorização dos seus progenitores ou de quem legalmente represente o menor, o que não acontece com os cidadãos maiores de idade.

Nas duas subsecções seguintes analisaremos os portais orientados a eventos da vida (portais OEV), e a composição de serviços OEV.

2.1.5.1 Portais orientados a eventos da vida (OEV)

Como vimos na secção anterior, o objetivo dos balcões únicos é concentrar a oferta de serviços da AP num único local por forma a facilitar o acesso dos cidadãos a esses serviços. No caso concreto da vertente que nos interessa, da oferta de serviços através da Internet, o conceito de balcão único concretiza-se no portal único (*one-stop portal*). No entanto, toda esta concentração de serviços pode criar dificuldades ao cidadão impedindo-o de encontrar facilmente o(s) serviço(s) de que necessita. Assim, além da segmentação da oferta em portais orientados para públicos-alvo, nos portais orientados para o cidadão foi sendo gradualmente adotado o modelo de organização da oferta de serviços públicos de acordo com eventos da vida[8] (United Nations 2012), ou seja, foram-se transformando em portais orientados a eventos da vida (*Life Event Portals*) (Vintar et al. 2002).

Uma característica dos eventos da vida é que normalmente requerem a obtenção de vários serviços públicos, possivelmente prestados por diferentes instituições. Estas instituições podem ser instituições públicas, por exemplo organismos da AP ou do Poder Local, ou instituições privadas, como companhias de seguros, bancos, notários, ou outras empresas prestadoras de serviços. Por exemplo, o evento da vida 'Compra de uma Casa' envolve interações com organismos da AP (e.g. a Conservatória do Registo Predial e as Finanças, entre outros) e com instituições privadas (e.g. bancos e notários). Isto requer do cidadão o conhecimento de quais os serviços que deve obter, quais as instituições que os

[8] Nos portais orientados para as empresas, usa-se um conceito semelhante que é a organização dos conteúdos de acordo com episódios de negócio (*business episodes*).

fornecem, qual a sequência pela qual devem ser obtidos, e o que é necessário para os poder obter (Vintar et al. 2002).

Os portais OEV partem do princípio de que o cidadão identifica bem o evento da vida que pretende satisfazer, mas não conhece nada sobre a organização da AP, pelo que tem dificuldade em identificar quais os serviços públicos que necessita e quais as instituições que os prestam (Todorovski et al. 2006). Subdividem-se em dois tipos de portais (Vintar et al. 2002): os portais passivos (*Passive Life Event Portals*) e os ativos (*Active Life Event Portals*). Os portais passivos atuam ao nível da organização dos conteúdos, i.e., os conteúdos, informação e apontadores para serviços, são organizados de acordo com os eventos da vida a que se referem e independentemente das instituições que prestam os serviços.

Antes de abordar os portais ativos, importa relembrar a definição de evento da vida em (Momotko et al. 2006): "*um evento da vida é um conjunto de ações personalizado, incluindo pelo menos um serviço público, que, quando executado num workflow apropriado, satisfaz uma necessidade do cidadão resultante de uma situação da sua vida*". Esta definição de evento da vida, que se enquadra no que convencionámos designar por um serviço OEV, refere dois aspetos importantes: um primeiro aspeto é a personalização, isto é, o conjunto de serviços públicos a obter para a satisfação de um determinado evento da vida depende de circunstâncias específicas do cidadão, o que, para diferentes cidadãos, pode significar diferentes conjuntos de serviços públicos. Por exemplo, no serviço OEV para a compra de uma casa apenas é necessária a participação de um banco se o cidadão decidiu recorrer ao crédito bancário. Um segundo aspeto é a existência de um *workflow.* Um *workflow* é a automatização de um processo de negócio, no seu todo ou em parte, usando computadores (Hollingsworth 1995), sendo um processo de negócio uma série de passos, atividades discretas, associados a operações humanas e/ou computorizadas e a regras que governam a progressão através dos vários passos (Hollingsworth 1995). Ou seja, a obtenção de um serviço OEV obedece a uma determinada ordem ou sequência de ações, derivada de interdependências entre elas, que deve ser seguida para se satisfazer o evento da vida (Trochidis et al. 2006). Por exemplo, no serviço OEV para a compra de uma casa, a escritura pública de compra e venda apenas pode ser realizada se um conjunto prévio de requisitos se verificar, que se manifestam num conjunto de atividades, como é o caso do pagamento do imposto IMT (Imposto Municipal sobre as Transmissões Onerosas de Imóveis), da realização do registo provisório, etc.

Os portais ativos não se limitam à organização de conteúdos e atuam no sentido de ajudar o cidadão a resolver o seu evento da vida. Essas ações enquadram-se nos dois aspetos dos serviços OEV mencionados no parágrafo anterior e são: (i) o diálogo com o cidadão no sentido de determinar quais são exatamente os serviços que ele deve obter em função das suas circunstâncias particulares (Vintar et al. 2002; Leben & Bohane 2004), e (ii) a composição num único serviço, o serviço OEV, dos vários serviços públicos que o cidadão necessita (serviços parciais), cuja execução de acordo com um processo adequado satisfaz o evento da vida do cidadão (Vintar et al. 2002; Pappa & Makropoulos 2004; Momotko et al. 2007). Estes dois aspetos vão também ser explorados no nosso trabalho, ainda que não no contexto de portais.

2.1.5.2 Composição de serviços OEV

Um aspeto importante para a disponibilização de serviços OEV é a composição do serviço, que é o processo de combinar múltiplos serviços (serviços parciais) num novo serviço composto (Dustdar & Papazoglou 2008). A composição envolve a seleção de quais os serviços parciais que vão ser usados e a elaboração de um plano ou sequência para a sua obtenção, e.g. um *workflow*, uma vez que normalmente existem dependências entre serviços.

A composição de serviços é uma característica do paradigma SOA (*Service Oriented Arquitecture*), no qual os serviços são usados como componentes para a construção de aplicações distribuídas e em ambientes heterogéneos. A composição pode ser estática (*static composition*) ou dinâmica (*dynamic composition*) (Marconi & Pistore 2009; Silva 2011; Sheng et al. 2014). No primeiro caso, a composição é feita em tempo de desenho, sendo o serviço primeiro composto e só depois disponibilizado para execução. O serviço composto é estático, no sentido em que não permite alteração de componentes em tempo de execução. Por oposição, a composição dinâmica de serviços permite a alteração de componentes em tempo de execução, pelo que tem de suportar a descoberta, seleção e a ligação a serviços componentes. A composição estática não se enquadra neste trabalho, pelo que não será mais referida.

Por outro lado, a composição de serviços pode ser manual, automática ou semiautomática (Marconi & Pistore 2009; Silva 2011; Sheng et al. 2014). Na composição manual, cria-se um modelo abstrato do serviço, que tipicamente é convertido para um processo abstrato descrito em linguagens como BPEL (*Business Process Execution Language*) (OASIS 2007) ou OWL-S (Semantic Web Ontology Language) (Martin et al.

2007), ao qual são depois ligados os serviços a usar. A composição automática baseia-se na utilização de tecnologias como a Web Semântica (*Semantic Web*) (Berners-Lee et al. 2001) e Inteligência Artificial para, dado um requisito, selecionar de um conjunto de potenciais serviços aqueles que melhor se adequam a satisfazer o requisito. Quanto à composição semiautomática, ela exige alguma intervenção humana, por exemplo para, de entre um conjunto de vários serviços que ofereçam a mesma funcionalidade, o utilizador selecionar aquele que pretende usar.

A composição do serviço pode ser feita por um especialista, pelo utilizador final ou por ambos. No primeiro caso é um especialista da área de negócio em que o serviço se insere que, com base num conjunto de requisitos, usa o seu conhecimento para determinar quais os serviços parciais que devem compor o serviço OEV e os combina de forma a satisfazer os requisitos. No segundo caso é o utilizador final que, de raiz, seleciona os serviços parciais e os compõe, de forma a satisfazer as suas necessidades específicas. No terceiro caso, o utilizador final talha ou adapta um serviço previamente composto (e.g. por um especialista), de forma a adequá-lo às suas necessidades (Silva 2011).

Na nossa pesquisa de soluções de composição dinâmicas para a prestação de serviços OEV, encontrámos composição semiautomática de serviços OEV, baseados em *workflows* (Tambouris et al. 2008; Dais et al. 2008), na Web Semântica (Gugliotta et al. 2005; Bednar et al. 2008; Sroga 2008; Sanati & Lu 2009; Feldkamp et al. 2010) e em tecnologias Web 2.0 (Dais et al. 2009; Dais et al. 2011). Em relação à execução do serviço composto, ela é sempre realizada numa plataforma que não está sob controlo efetivo do cidadão mas sim sob controlo da instituição que o disponibiliza, e.g. em portais ativos orientados a eventos da vida (Momotko et al. 2007). A razão para isto é que se considera que o cidadão utiliza apenas o seu navegador para obter os serviços pretendidos. No entanto, a tecnologia *Mashups* (Merrill 2009), uma das tecnologias da designada Web 2.0, que será analisada na secção 2.4.3, pode vir a permitir que o cidadão componha os serviços na sua plataforma. Mas um estudo de 2012 sobre a utilização de tecnologias Web 2.0 em iniciativas de governo eletrónico na Alemanha, França, Itália e Reino Unido (Gardini et al. 2012), detetou a utilização frequente de algumas destas tecnologias, mas não detetou a utilização de *Mashups*, o que comprova que a plataforma do utilizador não era utilizada, pelo menos nesses países, na composição de serviços.

2.1.5.3 Modelos de referência de serviços OEV

Os modelos de referência de serviços OEV, em particular os designados "*WHAT reference models*", são modelos abstratos e que servem como base de trabalho para o estudo e criação de serviços OEV. Nesta secção analisamos os modelos de referência para a modelação de serviços OEV, propostos por (Todorovski et al. 2007), porque introduzem alguns conceitos que iremos utilizar no modelo CHAPAS.

Os modelos de referência WHAT focam a modelação, baseada em *workflows*, dos serviços que o cidadão necessita para satisfazer o seu evento da vida, por oposição ao enfoque nos processos dentro desses serviços (visão funcional). Um conjunto destes modelos é proposto por (Todorovski et al. 2007) para servir como base para a integração de serviços públicos relacionados com virtualmente qualquer evento da vida, para vários níveis de abstração. Os níveis de abstração considerados são (i) o de um serviço específico, considerando as várias circunstâncias dos cidadãos que afetam o serviço final a obter pelo cidadão, (ii) o de um serviço específico mas a nível internacional (*cross country*), onde se consideram as especificidades de cada país na prestação de um mesmo serviço e (iii) um nível de abstração genérico, onde se propõe um modelo de referência geral para serviços OEV que permite a construção de modelos genéricos de virtualmente qualquer serviço OEV.

O modelo de referência geral para serviços OEV pode ser usado como molde (*template*) para a construção de *workflows* genéricos de virtualmente qualquer serviço OEV. Estes *workflows* designam-se genéricos porque devem incluir todas as circunstâncias passíveis de criar variações na prestação do serviço. A aplicação de um *workflow* genérico às circunstâncias específicas de um cidadão resulta num *workflow* específico, i.e, num *workflow* genérico do qual foram removidos todos os ramos que não se aplicam a esse cidadão em concreto.

Este modelo é de particular interesse para o nosso trabalho porque faz uma categorização dos vários tipos de serviços parciais que compõem um serviço OEV. Os tipos de serviços parciais identificados são três: serviços cruciais (*crucial services*), serviços de suporte (*support services*) e serviços complementares (*after-care services*). Tendo como base o exemplo do serviço público Casamento (*getting married*), usado pelo autor do modelo de referência geral, vamos fazer uma breve caracterização dos três tipos de serviços.

Serviços cruciais são serviços cuja obtenção é obrigatória para a satisfação do evento da vida. A sua obtenção tipicamente não está dependente de quaisquer circunstâncias do cidadão. Um exemplo de serviço crucial é o pedido de licença para casar (*applying for marriage*) que tem de ser obtido por todos os cidadãos que pretendam casar, quaisquer que sejam as suas circunstâncias. No entanto, as circunstâncias do cidadão podem afetar os documentos de entrada que o cidadão tem de fornecer para obter o serviço crucial. Por exemplo, dependendo se o cidadão for nacional ou estrangeiro, menor, viúvo ou divorciado, pode haver diferenças nos documentos que necessita de apresentar ao fazer o pedido de casamento.

Apesar de tipicamente os serviços cruciais serem de obtenção incondicional para a satisfação de um evento da vida, existem exceções em que tal não acontece. Por exemplo, no evento da vida "Perdi a minha carteira", a definição dos serviços cruciais a obter está dependente de quais em concreto foram os documentos perdidos. Um outro exemplo acontece no evento da vida "Quero viajar para o estrangeiro", em que a definição dos serviços cruciais, para obter documentos necessários para a viagem, depende do país em concreto para onde o cidadão pretende viajar, existindo casos em que é suficiente o documento de identificação civil, outros em que é necessário o passaporte e ainda outros em que é necessário o passaporte e um visto.

Serviços de suporte são serviços que se destinam a fornecer os documentos necessários para que o cidadão possa obter os serviços cruciais. Estes serviços podem ser muito numerosos e necessidade da sua obtenção está dependente das circunstâncias específicas do cidadão. Um exemplo de um serviço de suporte é a obtenção da autorização para o casamento de um menor, caso um dos noivos seja menor. Outros exemplos são a obtenção de documentos como um certificado de nascimento, a obtenção do documento de identificação civil, etc., caso o cidadão não os possua.

Serviços complementares são serviços opcionais que o cidadão pode invocar para complementar o serviço OEV já obtido. Exemplos de serviços complementares que podem ser necessários após um casamento são a mudança de nome e a mudança de morada. É de notar que a inclusão deste tipo de serviços nos eventos da vida não é consensual, por exemplo, não são incluídos no caso da Polónia (Todorovski et al. 2007).

Esta categorização de serviços parciais vai ser útil mais adiante para a composição de serviços OEV no modelo CHAPAS.

2.1.6 *INTEROPERABILIDADE*

A prestação de serviços integrados centrados no cidadão implica alguma forma de integração das instituições envolvidas na prestação desses serviços. No contexto do governo eletrónico, integração é a formação de um agrupamento de instituições, temporário ou permanente, com o objetivo de unir processos e/ou partilhar informação (Scholl & Klischewski 2007). Para que a integração possa acontecer é necessário descer ao nível técnico, i.e., ao nível da interoperação e interoperabilidade dos sistemas de informação das instituições envolvidas.

No contexto do governo eletrónico, interoperação ocorre sempre que sistemas de informação independentes ou heterogéneos controlados por diferentes instituições trabalham de forma efetiva em conjunto de acordo com um modo predefinido e acordado (Scholl & Klischewski 2007). Por sua vez, interoperabilidade refere-se à capacidade técnica para a interoperação (Scholl & Klischewski 2007), i.e., à "*capacidade de os sistemas de informação e comunicação, e dos processos de negócio por eles suportados, trocarem dados e possibilitarem a partilha de informação e conhecimento*"[9] (European Commission 2004).

A Comissão Europeia, através do *European Interoperability Framework* (EIF), definiu três níveis de interoperabilidade: técnica, semântica e organizacional (European Commission 2003a)[10]. Para cada um dos níveis define o que deve ser interoperável. Assim, a interoperabilidade ao nível técnico lida com questões relacionadas com a comunicação física entre sistemas; ao nível semântico lida com a uniformização de conceitos de forma a conseguir uma interpretação consistente dos dados por todas as entidades envolvidas; ao nível organizacional lida com a forma como as várias entidades cooperam para alcançar objetivos comuns, tais como a forma de relacionamento entre as entidades e o alinhamento dos respetivos processos de negócio.

---

[9] "*Interoperability means the ability of information and communication technology (ICT) systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge*".

[10] Posteriormente definiu um nível legal, acima do nível organizacional, que lida com a interoperabilidade a nível da legislação entre os vários países da União Europeia (European Commission 2010). Como neste trabalho não lidamos com aspetos legais, não nos pareceu relevante incluí-lo no conjunto dos níveis de interoperabilidade que considerámos.

Em 2006, o *European Telecommunications Standards Institute* (ETSI) definiu um nível adicional entre os níveis técnico e semântico, o sintático (Kubicek & Cimander 2009). Porém, este não foi adotado pelo EIF que o considera englobado no nível técnico. No entanto, salientamos a existência deste nível porque realça um aspeto importante que é o da normalização de formatos para a troca de dados.

A interoperabilidade tem sido gerida através de quadros de referência para a interoperabilidade, que definem o conjunto de regras que devem ser seguidas pelas várias instituições que pretendem colaborar entre si (European Commission 2008), como é o caso da já referida EIF, para a interoperabilidade a nível europeu, e do Guia Integração Eletrónica (Agência para a Modernização Administrativa 2011) para a interoperabilidade em Portugal.

Como exemplo de iniciativas com vista à interoperabilidade entre instituições, temos em Portugal a Plataforma de Interoperabilidade, também designada como Framework de Serviços Comuns (UMIC 2011). Nesta plataforma, ilustrada na Figura 1, os vários organismos da AP disponibilizam os seus serviços como *Web Services*, na camada de retaguarda, e os serviços para os utilizadores finais (cidadãos, empresas, funcionários, etc.) são oferecidos através de portais ou outras aplicações dos organismos, na camada de apresentação. A Plataforma de Interoperabilidade localiza-se entre as duas camadas atrás indicadas e disponibiliza serviços para a combinação de serviços e orquestração de processos, a autenticação e autorização eletrónicas, o pagamento de serviços e a privacidade, confidencialidade e segurança dos dados. A comunicação da Plataforma com os vários organismos é feita através de *Toolkits* que relacionam o modelo de dados usado na plataforma (modelo canónico) com os modelos de dados de cada organismo.

A interoperabilidade não é, contudo, fácil de alcançar. Kubicek & Cimander consideram que para a interoperabilidade aos níveis técnico e sintático já existem normas bem estabelecidas, como o TCP/IP, XML, EDIFACT, etc., o que permite considerá-los como completamente desenvolvidos (Kubicek & Cimander 2009). Já sobre o nível semântico, os mesmos autores consideram que já está bem definido no que diz respeito a aspetos teóricos, mas que ainda subsistem problemas em relação à sua concretização prática. Quanto ao nível organizacional, consideram que os conceitos que envolve ainda não estão suficientemente clarificados, pelo que é o nível em que é mais difícil alcançar interoperabilidade. Com efeito, têm sido identificados vários obstáculos ou barreiras à interoperabilidade (Lam 2005; Scholl & Klischewski 2007; Tambouris et al. 2008; Hellman 2010; Soares & Amaral 2011), referindo-se a maior parte deles à interoperabilidade ao

nível organizacional (Jaeger & Thompson 2003), como é o caso da resistência à mudança por parte das instituições, por exemplo, por temerem uma eventual perda de poder com a integração dos seus serviços (Lam 2005; Ebrahim & Irani 2005; Dada 2006; Howard 2014).

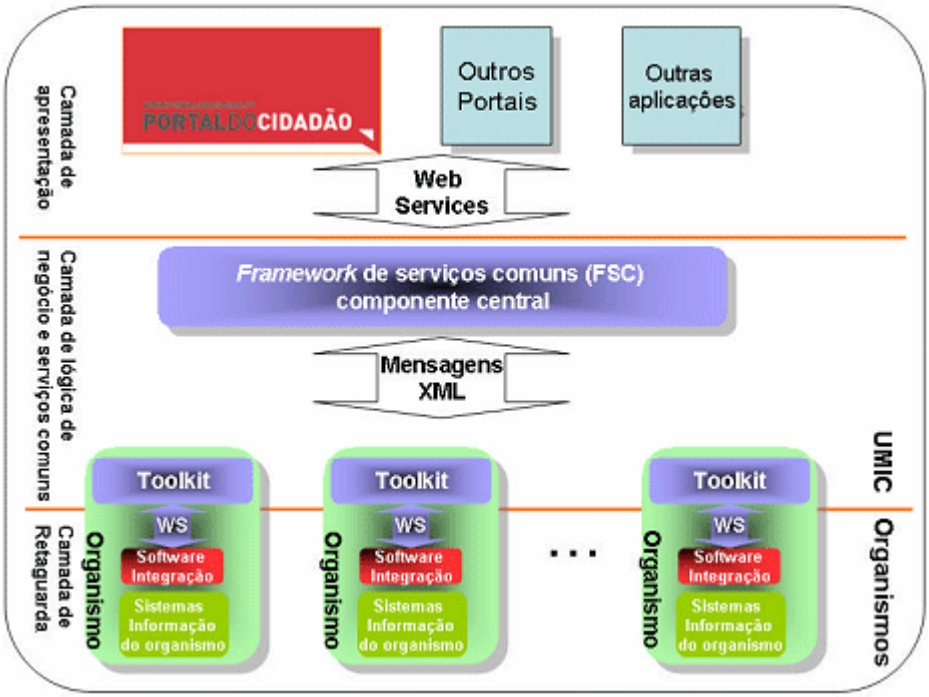

Figura 1: Plataforma de Interoperabilidade (UMIC 2011).

Os obstáculos à interoperabilidade levaram a Comissão Europeia a redefinir o seu conceito de interoperabilidade após reconhecer que existem mais do que apenas a fatores técnicos a influenciar a interoperabilidade (Novakouski & Lewis 2012). Assim, interoperabilidade passou a ser definida como "*a capacidade de instituições díspares e diversas de interagir para alcançar objetivos comuns acordados e com benefício mútuo, envolvendo a partilha de informação e conhecimento entre as instituições através dos processos de negócio por elas suportados, por meio da troca de dados entre os respetivos sistemas de informação e comunicação*" (European Commission 2010).

2.1.7 CONFIANÇA DO CIDADÃO NOS SERVIÇOS DO ESTADO

Como vimos, a prestação de serviços integrados implica alguma forma de integração da AP. A integração é mesmo, por vezes, apontada como o objetivo máximo a atingir com a evolução das iniciativas de governo eletrónico (Scholl & Klischewski 2007).

No entanto, a completa integração da administração pública não é assunto consensual e pode não ser desejável ou legal (Scholl & Klischewski 2007). Há mesmo quem argumente que a motivação para a integração da AP não é exclusivamente a prestação de melhores serviços aos cidadãos, mas sim a monitorização e o controlo de informação por parte do Estado (Yildiz 2007). Pelo contrário, a fragmentação da AP tem as suas vantagens do ponto de vista da preservação da privacidade os cidadãos (Bannister 2005).

A integração da AP tem inerente (i) a possibilidade de realização de processamentos de informação massivos, como a agregação, a partilha e a mineração, assim como (ii) a possibilidade de controlo, através da gestão centralizada e em tempo real da informação integrada. Vista de forma positiva, a integração cria as condições para a existência do diálogo e cooperação que permitem a resolução de problemas globais. Mas, vista de forma negativa, a integração pode ser encarada como um mecanismo para a repressão e o controlo e gerar a desconfiança por parte dos cidadãos (United Nations 2008). Ou seja, o problema da confiança do cidadão nos serviços de governo eletrónico surge devido ao conflito que existe entre a necessidade de se aceder a um maior conjunto de dados para se poder prestar melhores serviços e os receios das pessoas sobre segundas utilizações desses dados (Dutton et al. 2005).

A confiança dos cidadãos na prestação de serviços eletrónicos tem duas dimensões: (i) a confiança nas instituições ou, de forma genérica, no Estado, e (ii) confiança na Internet (Colesca 2009; Masrom et al. 2013). Esta segunda dimensão refere-se à confiança dos cidadãos de que as instituições possuem a capacidade de gestão e os recursos técnicos necessários para a prestação de serviços eletrónicos. A falha em qualquer uma destas dimensões da confiança coloca em causa a adesão aos serviços eletrónicos.

A primeira dimensão refere-se à confiança dos cidadãos nas boas práticas das instituições (de forma genérica, nas boas práticas do Estado) e é frequentemente apontada como uma barreira para a adesão do cidadão à prestação de serviços do governo eletrónico (Ebrahim & Irani 2005; Eynon 2007; Germanakos et al. 2007). Esta falta de confiança está muito associada a preocupações dos cidadãos com a sua privacidade, nomeadamente devido à facilidade de agregação de dados promovida pela integração dos serviços das instituições do Estado (Bannister 2005) e à perceção pelos cidadãos de que os seus dados pessoais podem ser comprometidos ou usados para segundas finalidades (Colesca 2009), mesmo que não seja essa a intenção da instituição a quem esses dados são confiados (Beldad et al. 2011). A falta de confiança dos cidadãos pode ainda agravar-se

devido à sensibilidade de alguma informação que o cidadão disponibiliza ao Estado, muitas vezes de forma compulsiva, e à falta de concorrência na prestação da maioria dos serviços do Estado (e.g., a coleta de impostos apenas é feita por uma única instituição: as Finanças), o que impede o cidadão de escolher a instituição que lhe inspire mais confiança (Beldad et al. 2012). Um exemplo claro desta falta de confiança dos cidadãos é fornecido pelo *Australian Government Information Management Office* que indica que a maioria dos australianos, nas suas várias interações com a AP através da Internet, prefere reintroduzir os seus dados pessoais a mantê-los armazenados nalgum organismo da AP (United Nations 2012).

Assim, para fomentar a confiança do cidadão é fundamental que as instituições garantam e demonstrem o cumprimento escrupuloso das boas práticas, i.e., que deem garantias da sua confiabilidade (Colesca 2009).

2.2 IDENTIFICAÇÃO DOS CIDADÃOS

A prestação de serviços do governo eletrónico implica frequentemente a identificação dos cidadãos que os pretendam obter, bem como o fornecimento de informação referente ao cidadão que pretende o serviço e/ou a outras pessoas. Isto é, a prestação de serviços lida com dados pessoais. Uma característica importante dos dados pessoais é que eles identificam a pessoa a que se referem. Por isso é de extrema relevância a forma como se lida com eles porque podem colocar em causa a privacidade das pessoas a que eles se referem.

Nas seguintes secções iremos fazer uma breve apresentação de conceitos sobre dados pessoais, privacidade e identidade.

2.2.1 DADOS PESSOAIS

Segundo a lei portuguesa, nomeadamente a Lei da Protecção de Dados Pessoais (Lei nº67/98 de 26 de Outubro de 1998), dados pessoais são "*qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável a pessoa que possa ser identificada directa ou indirectamente, designadamente por referência a um número de identificação ou a um ou mais elementos*

específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social" (Assembleia da República 1998). Esta lei decorre da transposição para a legislação nacional da diretiva nº 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Para a OCDE, dados pessoais "*são qualquer informação relacionada com um indivíduo identificado ou identificável (sujeito a quem os dados se referem).*"[11] (OECD 2013).

Já a Plataforma Terminológica Comum para a Gestão de Identidades Eletrónicas Interoperáveis da Comissão Europeia usa a expressão Informação Pessoalmente Identificável (*PII – Personally Identifiable Information*) para se referir a "*quaisquer dados que identifiquem ou se refiram a uma pessoa, natural ou legal, em particular*"[12] (Modinis-IDM 2005).

Na legislação americana, usa-se a expressão Informação Pessoalmente Identificável (PII) como equivalente à expressão europeia de Dados Pessoais (Kleek & Hara 2014) e refere-se a "*qualquer informação sobre um indivíduo mantida por uma agência do governo, incluindo (1) qualquer informação para distinguir ou rastrear a identidade de um indivíduo, tais como o nome, data e local de nascimento, nome de solteira da mãe, ou registos biométricos; e (2) qualquer outra informação que esteja ligada ou se possa ligar a um indivíduo, tais como informação médica, de educação, financeira e de emprego*"[13] (Mccallister et al. 2010).

Um aspeto relevante nas definições anteriores é que não há qualquer referência a qualidades da informação, como à sua eventual sensibilidade ou confidencialidade. Ou seja, não é o facto de uma informação ser sensível ou confidencial (e.g. informação médica) que faz com que seja qualificada como dados pessoais, ou informação pessoalmente identificável, mas sim o poder de identificar um individuo ou de se associar a um individuo.

---

[11] "*any information relating to an identified or identifiable individual (data subject)*".
[12] "*any data that identifies or refers to a particular natural or legal person*".
[13] "*any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information*"

Apesar de existirem algumas diferenças nas anteriores definições de dados pessoais e de informação pessoalmente identificável, elas não são relevantes para este trabalho. Assim, para evitar confusões, iremos apenas usar o termo dados pessoais, com a definição da OCDE, "*qualquer informação relacionada com um indivíduo identificado ou identificável (sujeito a quem os dados se referem)*", e com ele abarcar as anteriores definições.

Já a expressão "informação pessoal", por vezes é usada com um significado semelhante ao de dados pessoais, mas também é usada para significar um conjunto mais abrangente de informação, como é o caso de toda a informação que um indivíduo mantém para seu uso pessoal (Heikkinen et al. 2004; Al-Fedaghi & Taha 2006; Jones 2007), e que pode guardar no seu Gestor de Informação Pessoal (PIM – *Personal Information Manager*) (Bergman et al. 2004), o que além de dados pessoais pode incluir dados que não identificam nem permitem identificar o seu dono. Por essa razão evitaremos a utilização desta expressão e quando a usarmos será para significar toda a informação que pertence a uma pessoa, podendo incluir dados pessoais ou não.

Tendo em conta a definição de dados pessoais apresentada, muitos dos documentos que os cidadãos obtêm e fornecem no contexto da prestação de serviços de governo eletrónico são considerados dados pessoais porque contêm elementos que identificam ou permitem identificar as pessoas a que se referem.

Os dados pessoais são considerados o novo petróleo da Internet e a nova moeda do mundo digital (Kuneva 2009), o que ilustra o seu valor e importância. Com efeito, toda uma nova economia baseia-se na recolha e exploração dos dados pessoais, principalmente de utilizadores da Internet. Exemplos de grandes empresas nesta economia são a Google e o Facebook, entre outras. A recolha dos dados pessoais é por vezes feita sem que as pessoas se apercebam e outras vezes são os utilizadores que voluntariamente os fornecem em troca de algum serviço. O Estado, no conjunto de todos os seus organismos e níveis de poder, é também um grande coletor de dados pessoais (Vaz 2007), com a diferença de que muitos dos dados são recolhidos de forma compulsiva (os cidadãos são obrigados a fornecê-los) e/ou têm um grau de sensibilidade elevado.

Os dados pessoais são depois processados para a satisfação do objetivo da sua recolha, e eventualmente para outras utilizações secundárias (e.g., no caso de empresas privadas, para efeitos de marketing). Porém, o processamento dos dados pessoais, principalmente quando inclui o cruzamento de dados provenientes de diversas fontes, pode, por exemplo, revelar informação de carácter privado e de alta sensibilidade, como a

religião ou a saúde (Vaz 2007) ou perfis rigorosos de consumo, de identidade e de necessidades (Frois 2007), ou ser usado para manipular as emoções dos indivíduos (Kramer et al. 2014). Estes exemplos constituem claras violações da privacidade dos indivíduos e ilustram a importância da proteção dos dados pessoais.

2.2.2 PRIVACIDADE

O direito à privacidade dos cidadãos está consignado na Declaração Universal dos Direitos Humanos das Nações Unidas (United Nations General Assembly 1948), na Convenção Europeia de Direitos Humanos (Council of Europe 1950), bem como na Constituição de muitos países, como é o caso da portuguesa (Assembleia da República 2005). Este direito é depois regulado na legislação, como é o caso da já referida diretiva europeia da sobre a proteção de dados pessoais, diretiva nº 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, e da sua transposição para a legislação portuguesa, a Lei da Proteção de Dados Pessoais, a Lei nº67/98 de 26 de Outubro de 1998 (Assembleia da República 1998).

O estabelecimento de regras de proteção da privacidade é um processo que visa o equilíbrio entre a proteção do cidadão e outros interesses, e deve ter em conta três níveis (Westin 2003): (i) o político, (ii) o sociocultural e (iii) o pessoal. Ao nível político, consoante o tipo de regime, o ponto de equilíbrio entre as esferas pública e privada varia tendendo mais para a esfera pública nos regimes opressivos e mais para a esfera privada nos regimes democráticos. O nível sociocultural, uma vez que os comportamentos e atitudes socialmente aceitáveis variam de cultura para cultura e de sociedade para sociedade (Kemp & Moore 2007). Além disso, as diferenças entre vários estratos da população e as relações de poder que se estabelecem entre elas dão origem a diferentes necessidades de proteção da privacidade. O nível pessoal, porque cada indivíduo tem diferentes necessidades de privacidade em função da sua procura de equilíbrio psicológico. Estas necessidades podem ter grandes flutuações em função do ciclo de vida do indivíduo e de eventos que ocorram no dia-a-dia. Por exemplo, por vezes um indivíduo tem necessidade de se isolar completamente e não ser incomodado por outros, outras vezes precisa desesperadamente de desabafar com outras pessoas, eventualmente com desconhecidos que não o vão julgar. Entre estas duas situações extremas existe um grande conjunto de estados intermédios, mas o que importa realçar é que o nível de privacidade adequado em determinado momento é uma questão de escolha pessoal. A importância deste direito de escolha, tanto a nível do desenvolvimento pessoal como a nível do

exercício de cidadania, faz com que a exigência de privacidade seja uma parte fundamental da liberdade civil num regime democrático (Westin 2003).

Apesar da existência de um consenso sobre a importância da privacidade para o indivíduo, não há nenhum consenso sobre uma definição de privacidade (C. J. Bennett 2001). A privacidade é um conceito difícil de definir (Kemp & Moore 2007). É essencialmente um problema de relações humanas (Glazer & Blakley 2009) e fortemente contextual (Nissenbaum 2004). A discussão dos conceitos de privacidade pode ser feita em termos da linha fronteira entre o que é público e o que é privado, o que permite distinguir entre: (i) privacidade do espaço, (ii) privacidade do comportamento, (iii) privacidade das decisões e (iv) privacidade da informação. A privacidade do espaço baseia-se no conceito de que existe uma fronteira física entre o que é público e o que é privado. Por exemplo, a preocupação sobre os riscos para a privacidade devido ao uso de dispositivos biométricos encaixa-se na privacidade do espaço porque considera o espaço limitado do corpo humano. A privacidade do comportamento tem a ver com a esfera afetiva, com comportamentos, assuntos e ações íntimas como é o caso do amor, confiança e respeito no relacionamento com outras pessoas, por exemplo. A privacidade das decisões centra-se no direito de fazer escolhas sem interferências em relação a assuntos pessoais, como é o caso da contraceção, das crenças religiosas, etc. Em relação à privacidade da informação, o foco não está na necessidade de determinada informação ser inerentemente privada, mas sim no direito ao controlo da sua circulação. É este aspeto da privacidade que interessa em termos deste trabalho, pelo que as outras vertentes não serão mais abordadas.

Assim, do ponto de vista da informação, privacidade é o direito de um indivíduo a determinar quando, como, e que quantidade de informação sobre si é comunicada a outros (Westin 1967). Ou seja, privacidade não se refere à omissão ou ausência de informação, mas sim ao controlo que devemos ter sobre a informação que nos diz respeito (Glazer & Blakley 2009). Na definição de Westin, o controlo sobre a informação é limitado, uma vez que apenas se refere à divulgação da informação pela pessoa a quem ela se refere, mas essa informação pode ser armazenada e posteriormente partilhada e sujeita a múltiplos processamentos (Whitley 2009). Um indivíduo deve reter os seus direitos em relação aos seus dados pessoais, o que inclui o direito de lhe ser pedido o consentimento prévio para a partilha com outras entidades ou o processamento para outras finalidades (L. Bennett 2009).

As atividades suscetíveis de violar a privacidade de um indivíduo são muitas e de várias naturezas. Estas podem ser classificadas numa taxonomia, ilustrada na Figura 2, que inclui os seguintes grupos de atividades (Solove 2006): (i) recolha de informação, (ii) processamento de informação, (iii) disseminação de informação e (iv) invasões. Todos os tipos de atividades que afetam a privacidade, identificadas e incluídas em cada um dos grupos, são relevantes do ponto de vista da privacidade individual, mas destacamos as que se enquadram no processamento de informação, por estarem mais relacionadas com este trabalho. Assim, neste grupo incluem-se atividades como (i) a agregação, que se refere à combinação de vários dados sobre um indivíduo, (ii) a identificação, que se refere à associação de informação a indivíduos específicos, (iii) a insegurança, que se refere ao pouco cuidado na preservação da informação e que pode resultar em fugas de informação e em acessos indevidos, (iv) o uso secundário, que se refere à utilização da informação para finalidades diferentes daquela para a qual foi recolhida e sem o consentimento do individuo a quem ela se refere, e, por último, (v) a exclusão, que acontece quando um indivíduo não sabe que outros possuem informação sobre si e, por isso, não participa na sua manipulação e uso.

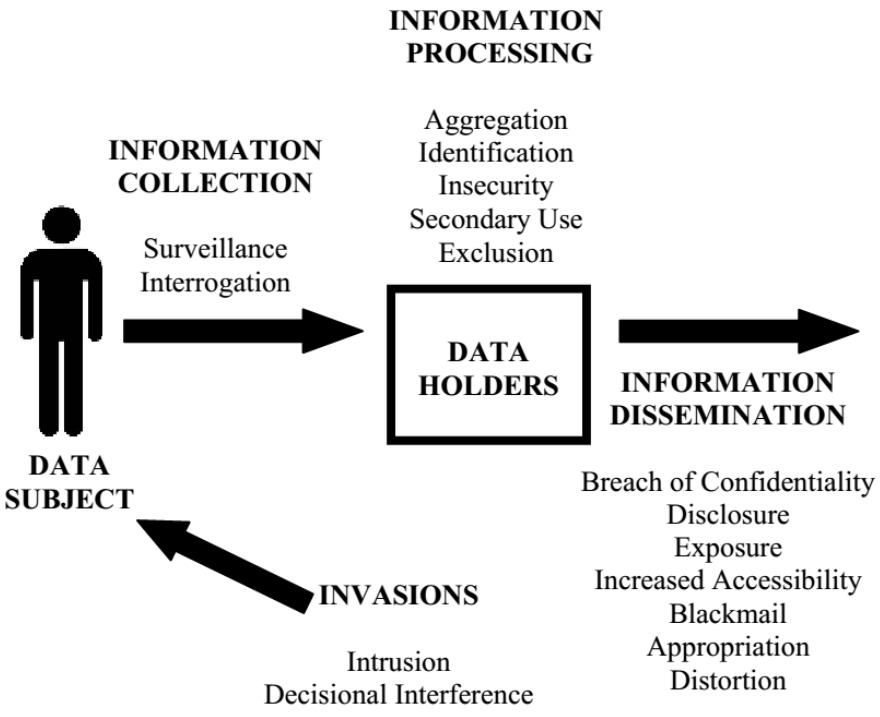

Figura 2: A taxonomia de atividades que afetam a privacidade (Solove 2006).

A agregação de informação é uma das atividades com um maior potencial de criar riscos para a privacidade dos cidadãos. Ela é feita através da junção de itens de informação de diversas fontes, por exemplo de diferentes bases de dados, usando como elementos de

ligação características (atributos) de identidade das pessoas (sobre características de identidade, ver secção 2.2.3) a que esses itens se referem. Esses vários itens de informação podem não ser relevantes *per se*, mas a sua junção pode criar perfis da pessoa a que se referem (Solove 2007). Trata-se de um caso em que o resultado é maior que a soma das partes. Para minimizar este cruzamento de dados, a divulgação de dados pessoais deve ser minimizada ao mínimo indispensável (Cameron 2005; Cavoukian 2006).

O Estado recolhe muita informação de cariz confidencial e por vezes de forma compulsiva (Alves & Moreira 2005; Lindgren & Jansson 2013). Por outro lado, as preocupações do cidadão com a privacidade crescem com a quantidade e a sensibilidade dos dados pessoais que fornece (Lindgren & Jansson 2013). Por essa razão, os serviços de governo eletrónico devem ser exemplares na proteção da privacidade dos cidadãos (Lau 2003). Além disso, o Estado tem o dever especial de agir de forma responsável e transparente, e de comprovar que o faz, em relação à recolha, processamento e eliminação de dados pessoais, de forma a criar confiança e fomentar a democracia (L. Bennett 2009).

Quanto às instituições privadas, o respeito pela privacidade dos utilizadores, para além de ser um dever ético, também pode trazer vantagens, como, por exemplo, ser capitalizado para criar uma boa reputação e ser usado como uma vantagem competitiva (Cavoukian 2013).

2.2.3 IDENTIDADE

Uma entidade é uma pessoa ou uma coisa caracterizada através da medida dos seus atributos (Modinis-IDM 2005). Um atributo é uma característica associada a uma entidade (Camp 2005) ou, de forma mais detalhada, um atributo é uma propriedade distinguível, mensurável, física ou abstrata, com um nome, que pertence a uma entidade, e que tem um valor (Modinis-IDM 2005). A título de exemplo, um cidadão é uma entidade que como atributos tem, por exemplo, um nome, uma cor dos olhos, uma morada, etc. Para um determinado cidadão, os valores dos atributos atrás indicados poderão ser, respetivamente, Hélder Gomes, castanhos e Aveiro, por exemplo.

Alguns dos atributos de uma entidade são persistentes, i.e., os seus valores nunca ou raramente mudam, como é o caso do nome e da data de nascimento de uma pessoa. Outros atributos são temporários ou de curta duração, podendo os seus valores variar frequentemente, como é o caso da morada, da idade, etc.

A identidade de uma entidade é o conjunto dinâmico de todos os seus atributos (Modinis-IDM 2005), que fazem com que ela seja quem é (Roundtree 2008). Este conceito de identidade é um conceito filosófico fluído, mais do que um conceito prático, uma vez que o número de atributos que caracterizam uma entidade é teoricamente ilimitado. Note-se que, conceptualmente, uma identidade não é obrigatoriamente exclusiva de uma entidade. Duas entidades dizem-se idênticas quando possuem a mesma identidade, isto é, todos os seus atributos são iguais (Fischer-Hübner & Hedbom 2008).

Uma entidade possui apenas uma identidade, identidade essa que varia ao longo do tempo de acordo com a variação dos valores dos seus atributos. Apesar de o conjunto de atributos de uma entidade poder não ser único, ele é sempre útil para ajudar a distinguir entre várias entidades (Modinis-IDM 2005).

Uma entidade pode ser uma qualquer coisa e não obrigatoriamente uma pessoa. No entanto, para facilitar a apresentação dos restantes conceitos vamos restringi-la apenas a pessoas, mas tendo sempre presente que esses conceitos são válidos para qualquer entidade.

2.2.3.1 Identidades parciais

As pessoas apresentam-se, comportam-se e reagem de formas diferentes dependendo do contexto em que se encontram e do tipo de interação em que participam. Isto é, divulgam diferentes subconjuntos dos seus atributos, o que faz com que sejam reconhecidas de diferentes formas (Roosendaal et al. 2009). Por exemplo, dificilmente uma mesma pessoa será caracterizada pelos seus colegas de trabalho da mesma forma que o será pelos seus amigos mais próximos. Esta diferente caracterização poderá envolver atributos diferentes ou mesmo valores diferentes para um mesmo atributo. Um subconjunto de atributos de uma entidade designa-se por identidade parcial (Modinis-IDM 2005) e normalmente representa essa entidade num determinado contexto ou papel (Cameron 2005; Cavoukian 2006; Fischer-Hübner & Hedbom 2008). A Figura 3, extraída do projeto Prime (Prime 2004), ilustra o conceito de identidades parciais de um indivíduo, o John.

2.2.3.2 Identidade digital

Os conceitos de entidade e de identidade também existem no domínio digital. Assim, uma entidade digital é uma entidade representada ou existente no domínio digital (Cameron 2005) e uma identidade digital é uma identidade parcial em formato eletrónico (Modinis-IDM 2005), ou um conjunto de atributos de uma entidade operacionalmente acessíveis por meios técnicos, como para armazenamento ou processamento por um programa de computador (Fischer-Hübner & Hedbom 2008). Note-se que uma identidade digital é sempre uma representação de uma identidade parcial, uma vez que, por definição, uma identidade é caracterizada pela totalidade dos seus atributos, que são em número ilimitado. Por esta razão, e porque é a representação digital de identidade que nos interessa, fazemos uma simplificação de terminologia e usamos o termo identidade como sinónimo de identidade digital. Sempre que pretendermos referir uma identidade na verdadeira acessão do termo, na sua totalidade, usaremos a expressão identidade completa.

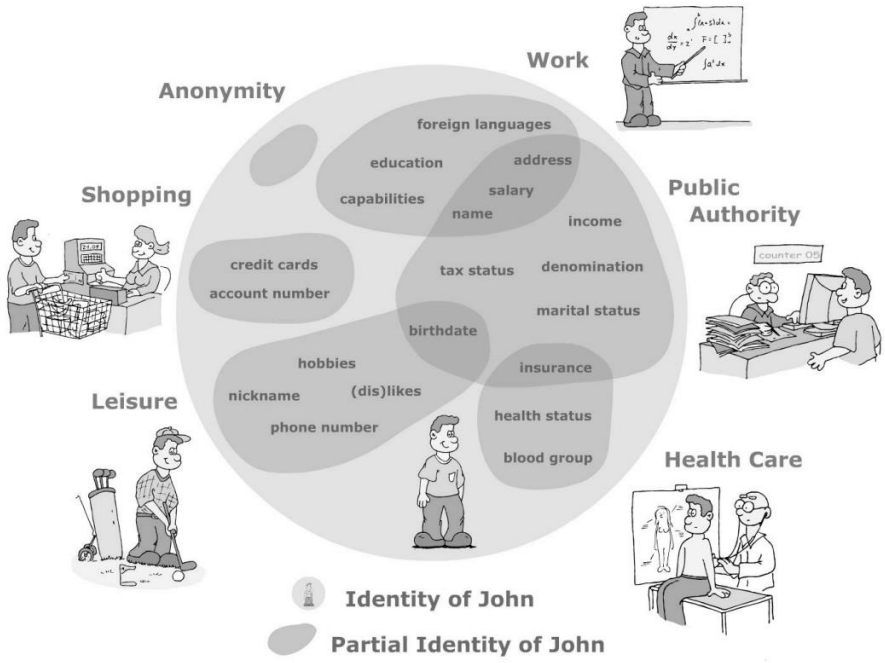

Figura 3: As múltiplas identidades parciais de um indivíduo (Prime 2004).

2.2.3.3 Identificador

No contexto do governo eletrónico uma identidade descreve ou distingue de forma única uma pessoa ou entidade (Camp 2005). Para garantir que não há duas entidades com uma mesma identidade são usados atributos especiais, os identificadores.

Um identificador é um atributo ou um conjunto de atributos de uma entidade que a identificam de forma única num determinado contexto (Modinis-IDM 2005). Ou seja, um identificador permite distinguir uma entidade específica no meio de um conjunto de entidades, uma vez que é suposto não haver duas entidades com o mesmo identificador, mesmo que os restantes atributos sejam iguais. Um identificador persistente é um identificador que se baseia num atributo persistente, i.e., cuja alteração é difícil ou impossível. Um identificador pessoal é um identificador persistente associado a uma pessoa natural (Camp 2005). Exemplos de identificadores pessoais são a Número de Identificação Civil, a impressão digital, o ADN, etc. Alguns dos identificadores baseiam-se em atributos naturais das pessoas (e.g. a impressão digital), enquanto outros são criados e impostos pelo Estado, como é o caso dos números de identificação (Raab 2005).

Além dos identificadores, o Estado estabelece mais um conjunto de atributos persistentes para auxiliar na definição da identidade dos cidadãos (para outras entidades, como empresas, estabelece outro conjunto de atributos). Estes atributos são persistentes para que a identidade seja estável ao longo do tempo, condição necessária para a emissão de documentos de identificação (Camp 2005). Exemplos de atributos usados para definir a identidade do cidadão são o nome, a morada, a data de nascimento, etc.

Nalguns países, os cidadãos tem um identificador único que os identifica em todas as interações com o Estado. Noutros países, como é o caso de Portugal, cada cidadão tem vários identificadores estabelecidos pelo Estado, estando cada um associado a um organismo específico, como acontece com o Número de Identificação Fiscal que identifica o cidadão perante as Finanças, o Número da Segurança Social, que identifica o cidadão nas interações com a Segurança Social, etc. Ou seja, o cidadão tem em simultâneo e em paralelo várias identidades para o seu relacionamento com o Estado e estabelecidas por este (Lips 2010).

2.2.3.4 Identificação

A identificação de uma entidade é o processo de utilização de atributos da mesma, observados ou reivindicados (*claimed*), para deduzir quem é essa entidade (Modinis-IDM 2005). Atributos reivindicados são atributos que a pessoa a identificar apresenta e reivindica (*claims*) como sendo seus, e atributos observados são atributos da entidade a identificar que a entidade identificadora pode observar diretamente. A identificação da entidade A pela entidade B ocorre quando a entidade B compara um conjunto de atributos de A com os valores previamente guardados desses mesmos

atributos e verifica que são coincidentes (Lips et al. 2010). Ou ainda, trata-se de associar um identificador pessoal a um indivíduo que apresenta um conjunto de atributos (Camp 2005), como por exemplo associar um nome a uma pessoa: "tu és o Hélder".

Uma reivindicação (*claim*) é definida como uma asserção sobre a verdade de alguma coisa, tipicamente algo que esteja a ser disputado ou em dúvida (Cameron 2005). Esta definição indicia que a decisão de aceitar uma reivindicação como verdadeira cabe a quem a avalia e não a quem a apresenta. Isto é, quando uma pessoa A se identifica dizendo o seu nome a uma outra entidade B, está a reivindicá-lo como sendo seu e verdadeiro, mas a decisão de o aceitar como verdadeiro não lhe cabe a ela (A), mas sim a B que é quem a está a identificar. A utilização do termo reivindicação torna claro que uma entidade reivindica mas é a outra entidade que avalia e decide se aceita ou não a reivindicação apresentada.

O conjunto de atributos a usar na identificação de uma entidade é variável consoante o contexto em que a identificação ocorre. Por exemplo, para um cidadão se identificar perante a Justiça tem de apresentar um conjunto de atributos como o Número de Identificação Civil, o nome, a morada, data de nascimento, etc. Mas para se identificar uma pessoa num grupo de amigos normalmente basta o nome e em caso de ambiguidade alguma outra característica particular, como a cor do cabelo, altura, etc. Mais, existem contextos em que as identidades nem sequer precisam de ser únicas. Por exemplo, num cenário em que apenas é permitida a venda de bebidas alcoólicas a indivíduos de maior idade, um comprador não necessita de apresentar um conjunto de atributos que o individualize em relação ao resto da população, mas apenas que demonstre a sua elegibilidade para poder efetuar a compra, i.e., que tem pelo menos 18 anos de idade.

2.2.3.5 Autenticação

A autenticação está intimamente associada à identificação e permite que uma entidade prove a sua identidade. É o processo de estabelecimento de confiança nas identidades digitais dos interlocutores (Burr et al. 2008). Permite garantir que uma entidade é quem reivindica ser (Lips et al. 2010). É ainda a prova de um atributo (Camp 2005). É através da autenticação que uma entidade prova a veracidade de uma reivindicação que apresenta a outra entidade.

A autenticação é de extrema importância para a tomada de decisões sobre permissões de acesso a recursos, i.e., controlo de acessos. Com efeito, a autorização para o

acesso a um determinado recurso por parte de uma entidade, está dependente de uma prévia determinação, com um nível de confiança adequado, da identidade da entidade que pretende aceder ao recurso, i.e., de uma prévia autenticação dessa entidade. Conhecendo-se a identidade da entidade pode-se então verificar se tem ou não o direito de acesso ao recurso pretendido e, consoante o caso, permitir ou negar esse acesso.

A autenticação de uma entidade passa invariavelmente pelo fornecimento de uma prova da sua identidade (uma prova de que ela é quem afirma ser). Esta prova pode ser de várias naturezas (fatores de autenticação): algo que se sabe, algo que se possui ou algo que se é (Smith 2001).

Em termos da autenticação dos cidadãos no acesso a serviços de governo eletrónico a autenticação é cada vez mais realizada através de dispositivos *smartcard* (ENISA 2009), como é o caso do Cartão de Cidadão em Portugal[14]. Estes cartões incorporam funcionalidades criptográficas que permitem a geração de chaves assimétricas e a realização de operações de criptografia assimétrica no interior do cartão, nomeadamente a assinatura digital. Além disso, estão desenhados de forma que as operações criptográficas apenas possam ser realizadas após a introdução de um PIN de proteção e de forma a impedir a exportação das chaves privadas para o exterior. A sua utilização é feita no contexto de Infraestruturas de Chave Pública (PKI – *Public Key Infrastructure*), que emitem certificados digitais de chave pública que associam a identidade do cidadão dono do cartão (um conjunto de atributos de identidade) com a chave pública correspondente à chave privada dentro do cartão. Esta associação permite que o cidadão se autentique realizando operações criptográficas envolvendo a chave privada, assinaturas digitais, para o que necessita de estar na posse do cartão e ter conhecimento do PIN de proteção (multifator). A correspondente verificação pode ser feita por qualquer entidade, utilizando o certificado digital para validar a assinatura e para obter a identidade do cidadão que a produziu, desde que confie no certificado e na entidade (PKI) que o emitiu.

[14] http://www.cartaodecidadao.pt

2.2.3.6 Gestão da identidade

A gestão de identidades digitais refere-se ao estabelecimento e ao uso controlado de identidades no mundo digital (Windley 2005). As leis da identidade (Cameron 2005) definem um conjunto de princípios que devem ser seguidos para uma gestão da identidade cuidada e respeitadora da privacidade (Cavoukian 2006). Um destes princípios é a minimização da divulgação de atributos de identidade, i.e., divulgar apenas os atributos necessários para o contexto em que vão ser usados, com base na "necessidade de saber" (*need to know*), e apenas às entidades que de facto necessitam deles (Bauer 2009). Inclusive, em muitas operações não há nenhum objetivo especial para associar uma determinada informação a um indivíduo, sendo aceitável a utilização de pseudónimos ou mesmo a sua realização de forma anónima (Shroff & Fordham 2010).

Em linguagem comum, um pseudónimo é um nome diferente do nome real de uma pessoa. A sua utilização é comum em artistas das mais variadas áreas, frequentemente para dissociarem a sua vida pública da sua vida privada e dessa forma garantirem a sua privacidade. Em termos mais precisos, um pseudónimo é um identificador de uma entidade que não é um identificador real (Pfitzmann & Hansen 2009). Os pseudónimos podem ser usados de forma persistente ou de forma descartável. Quando uma entidade usa pseudónimos descartáveis consegue um maior grau de privacidade uma vez que pode não ser fácil ou possível fazer a agregação das várias utilizações por os identificadores serem diferentes. A utilização de pseudónimos persistentes permite a agregação das várias utilizações que tiveram, ainda que não se consiga associar essas utilizações a uma identidade verdadeira.

Uma entidade está anónima quando não é identificável dentro de um conjunto de entidades (Pfitzmann & Hansen 2009). Ou seja, implica a existência de um conjunto apropriado de entidades todas com potencialmente os mesmos atributos.

2.3 ARQUITETURA ORIENTADA A SERVIÇOS (SOA)

Nesta secção vamos fazer uma breve apresentação do conceito de Arquiteturas Orientadas a Serviços (SOA – *Service Oriented Architecture*), fundamental para a prestação de serviços integrados.

SOA é um estilo arquitetural, tecnologicamente neutro, que organiza funcionalidades discretas em unidades lógicas (serviços) autónomas, mas não isoladas, interoperáveis e normalizadas, que podem ser combinadas e reutilizadas para satisfazer uma necessidade de negócio (Davis 2009). De acordo com a W3C, uma arquitetura SOA "*é um conjunto de componentes independentes que podem ser invocados e cujas descrições das respetivas interfaces podem ser publicadas e pesquisadas*"[15] (Haas & Brown 2004). Ou seja, SOA é um paradigma que fomenta a disponibilização de serviços autónomos (*loosely coupled*) por parte das várias instituições, que podem depois ser usados e combinados para a criação de novos serviços.

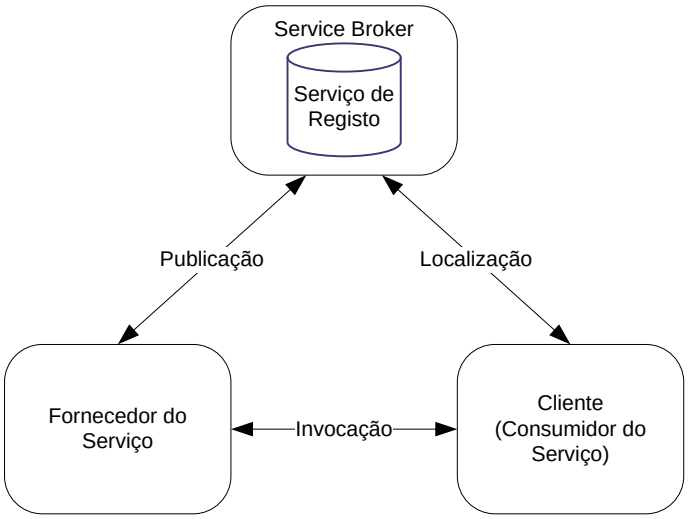

Figura 4: Modelo de Interação SOA.

A exploração de SOA baseia-se num modelo de interação entre três entidades principais, ilustrado na Figura 4, que são: (i) o Fornecedor do Serviço (*Service Provider*) que publica a descrição do serviço e disponibiliza uma instanciação do serviço, (ii) o Consumidor do Serviço (*Service Consumer*), ou Cliente, que localiza e obtém a descrição do serviço num Serviço de Registo (S*ervice Registry*), e a usa para o invocar, e (iii) um *Service Broker* que disponibiliza e gere um Serviço de Registo, não sendo esta entidade obrigatória.

[15] "*A set of components which can be invoked, and whose interface descriptions can be published and discovered*".

2.3.1 *WEB SERVICES*

A SOA, apesar de ser tecnologicamente neutra, está fortemente associada à tecnologia de *Web Services* (Erl 2005). Um *Web Service* é uma aplicação que é disponibilizada na Web, através de um URI, cujas capacidades e *modus operandi* são descritas em XML e que é capaz de comunicar usando mensagens em XML (Bray et al. 2006) sobre um protocolo de transporte (Benatallah et al. 2005). Segundo a W3C, um *Web Service* é "*um sistema de software desenhado para suportar interações interoperáveis entre máquinas (machine-to-machine) sobre uma rede. Possui uma interface descrita num formato processável por máquinas (machine processable) (nomeadamente, a Web Service Definition Language, WSDL* (E. Christensen et al. 2001; Booth & Liu 2007)*). Os outros sistemas interagem com o Web Service usando mensagens SOAP* (Mitra & Lafon 2007) *de acordo com o prescrito na sua descrição, tipicamente transportadas usando HTTP com uma serialização XML em conjunto com outras normas Web relacionadas*"[16] (Booth et al. 2004).

Um *Web Service* pode ser encarado como a instanciação de uma funcionalidade (serviço) definida num contrato (Erl et al. 2009). Este contrato, referido como *Service Description* na Figura 5, contém meta-dados sobre o serviço, sendo a sua parte fundamental composta por documentos que expressam a interface técnica do serviço, os quais são: (i) a definição do WSDL, que especifica a interface do serviço e a sua implementação, (ii) a definição dos esquemas XML (XML *schemas*) (Fallside & Walmsley 2004) dos dados trocados nas mensagens entre o serviço e os clientes, e (iii) a definição de políticas (WS-Policy) (Vedamuthu et al. 2007) que devem ser satisfeitas pelos clientes para poderem aceder ao serviço. Por cada serviço tem de existir um único documento com a definição do WSDL, que pode incluir a definição dos esquemas dos dados trocados nas mensagens e a definição de políticas.

É de notar que é irrelevante qual a tecnologia usada na implementação do serviço, desde que este cumpra o que está estabelecido no contrato, uma vez que vai ser no contrato que as aplicações cliente se vão basear para interagir com o serviço.

[16] *"A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP-messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards."*

Adicionalmente, o contrato pode também incluir documentos para consumo humano, que não são relevantes no contexto deste trabalho.

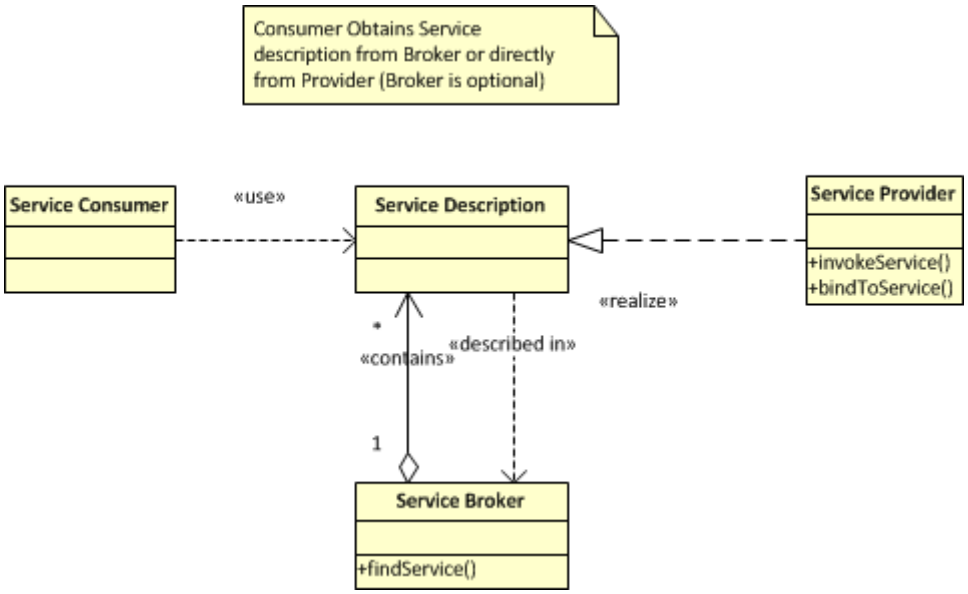

Figura 5: Implementação do modelo de interação SOA (Arsanjani et al. 2004)

O WSDL é uma linguagem para descrever *Web Services*, baseada em XML, mas cujo nome foi também adotado para referir o documento que contém a descrição do *Web Service*, o que também faremos daqui em diante (designando-o apenas por WSDL ou documento WSDL). O WSDL de um *Web Service* é tipicamente disponibilizado no endereço onde o serviço é disponibilizado, acrescentado de "`?wsdl`", como em `http://www.pservicos.pt/servico1?wsdl`, por exemplo.

O contrato de um serviço visa essencialmente responder a três questões sobre a interface técnica deste: (i) o que é que o serviço faz (*What*)?; (ii) como é que se pode aceder ao serviço (*How*)?; e (iii) onde é que se pode aceder ao serviço (*Where*)?

A resposta à primeira questão constitui aquilo que se designa como a descrição abstrata da interface técnica, isto é, descreve a interface de forma independente de detalhes de implantação. A interface é expressa em termos de operações que podem ser solicitadas, as mensagens que compõem cada operação, que podem ser de três tipos: de entrada, de saída e de sinalização de falha, e a estrutura de cada mensagem (tipos de dados).

As respostas à segunda e terceira questões constituem a designada descrição concreta da interface técnica, onde são descritos os aspetos de implantação do *Web*

Service. Nomeadamente, define qual o formato das mensagens, o protocolo de transporte a usar (*binding*) e qual o endereço onde o serviço pode ser obtido.

Tanto a descrição abstrata como a descrição concreta descrevem essencialmente os aspetos funcionais da interface técnica. Estas podem ser complementadas com a definição de políticas para exprimir requisitos não funcionais (comportamentais) e características do serviço. A norma que define como se incorpora a definição de políticas no WSDL é a norma *WS-Policy* (Vedamuthu et al. 2007), existindo depois normas para políticas específicas, como a norma *WS-SecurityPolicy* (Nadalin et al. 2009) que define como expressar políticas de segurança. A norma *WS-Policy* permite também a utilização de políticas definidas pelas aplicações e não sujeitas a normalização.

2.3.2 INTERAÇÕES EM WEB SERVICES

Como vimos na secção anterior, a interface dos *Web Services* é expressa em termos de operações que são compostas por mensagens que fluem nos dois sentidos, de e para o *Web Service*. Para tipificar o fluxo das mensagens, a norma WSDL prevê a existência de padrões de troca de mensagens (MEP – *Message Exchange Patterns*), definindo quatro padrões básicos, tendo como referência o papel do servidor (Erl et al., 2009). São eles:

(i) o padrão pedido-resposta (request-response), em que o servidor recebe uma mensagem com um pedido e envia uma mensagem com a respetiva resposta;

(ii) o padrão sentido único (One-Way), em que o servidor recebe uma mensagem com alguma informação e não envia nenhuma mensagem de resposta;

(iii) o padrão solicitação-resposta (Solicit-Response), em que o servidor toma a iniciativa de enviar uma mensagem para um cliente e recebe uma outra mensagem com a resposta;

(iv) o padrão notificação (Notification), em que o servidor envia uma mensagem com alguma informação a um cliente e não é suposto haver resposta.

Estes quatro padrões de interação são simples e de modo nenhum esgotam todas as possibilidades de interação de *Web Services*. Assim, é possível ter como base estes padrões e combiná-los de modo a definir outros mais elaborados que satisfaçam as

necessidades concretas de interação entre/com *Web Services* no contexto de alguma aplicação.

2.4 APLICAÇÕES QUE REFORÇAM O CONTROLO PELO UTILIZADOR

Nesta secção vamos analisar três tipos de aplicações que permitem ao utilizador o reforço do controlo sobre os seus dados ou sobre os serviços que pretende. São elas: os *Electronic Data Safes*, os *Card Selectors* e os *Mashups*.

Uma característica destas aplicações é que podem ser executadas em plataformas do utilizador, tal como o Chappie, a aplicação do cidadão no modelo CHAPAS. Além disso, lidam com dados pessoais do utilizador (os *Electronic Data Safes* e os *Card Selectors*), ou podem lidar (os *Mashups*), pretendem colocar o cidadão no controlo do fluxo da sua informação (os *Electronic Data Safes* e os *Card Selectors*) e podem ser usadas para obter serviços OEV (os *Electronic Data Safes* e os *Mashups*).

2.4.1 ELECTRONIC DATA SAFES (EDS)

Com o termo *Electronic Data Safes* (EDS) abarcamos um conjunto de conceitos semelhantes, como os *Personal Data Lockers*, *Personal Data Stores* e *Personal Data Vaults* (Pfister & Schwabe 2013). Um EDS é um componente do conceito de *Personal Data Ecosystem* (PDE) segundo o qual, a informação pessoal de um indivíduo é um recurso do próprio, controlado pelo próprio indivíduo, que este pode usar para melhor organizar e gerir a sua vida (Cavoukian 2012). Outras motivações para o PDE são (i) a crescente tendência para os governos devolverem aos cidadãos os seus dados, como é o caso das iniciativas Midata (I. S. Group 2013), no Reino Unido, e BlueButton[17] (Cavoukian 2012), nos Estados Unidos; (ii) o fomento da qualidade e confiança nos dados dos indivíduos, requisito importante para muitas empresas (Mydex 2010), e (iii) fazer com que o indivíduo participe na exploração e distribuição do valor económico da sua informação

[17] http://www.va.gov/BLUEBUTTON/

pessoal, evitando a exploração exclusiva pelas empresas que a têm na sua posse (Kirkham et al. 2013).

Um EDS é um armário (*locker*) virtual baseado em tecnologias da informação e comunicação onde um utilizador agrega toda a sua informação pessoal e a explora para seu uso pessoal e partilha com entidades terceiras de acordo exclusivamente com os seus interesses (Pfister & Schwabe 2013).

O objetivo do EDS é ajudar os indivíduos na recolha, armazenamento, partilha e gestão da sua informação pessoal, incluindo dados estruturados e não estruturados, tais como texto, imagens, vídeo e som (Cavoukian 2012). A informação pessoal do utilizador reside no seu EDS, em vez de residir espalhada por diversas organizações (ver Figura 6), que fornece ao utilizador um ponto central de controlo para a sua informação pessoal. Conceitos chave no EDS são o "*controlled push*" e o "*informed pull*"(Cavoukian 2013), que permitem ao utilizador fornecer informação pessoal de forma controlada e também pedir dados de outras fontes, de acordo com os seus próprios critérios.

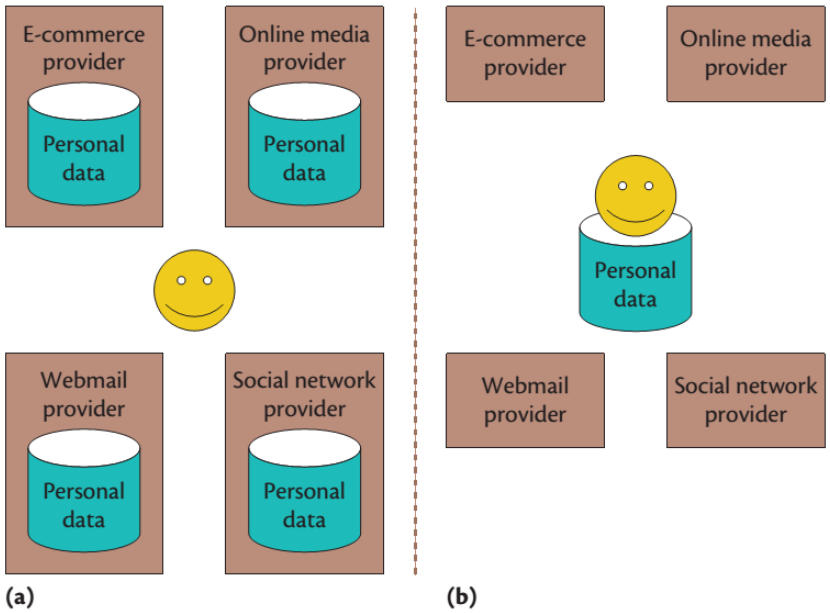

Figura 6: Comparação entre os modelos de armazenamento de informação pessoal em (a) aplicações tradicionais e (b) com *Electronic Data Safers*. Neste segundo modelo, é o indivíduo que mantêm os seus dados pessoais na sua EDS, e que controla, de acordo com os seus interesses, o acesso a eles por parte das aplicações (Kirkham et al. 2013).

O EDS pode residir num único local ou estar distribuído, assim como pode ser albergado pelo próprio utilizador ou por uma empresa hospedeira que atua como agente de dados pessoal (*personal data agent*) com a obrigação de representar os interesses do indivíduo na partilha e utilização dos seus dados. Esta obrigação deve estar consignada

legalmente nas regras de governação de um PDE, como acontece na Respect Trust Framework™, um mecanismo que permite que todas as partes numa federação fiquem obrigadas a um conjunto de regras técnicas e legais (Reed et al. 2011). Numa analogia entre informação pessoal e dinheiro, o *personal data agent* deverá agir como um banco, no qual os indivíduos depositam os seus dados pessoais. A gestão e o controlo das contas onde são depositados os dados pessoais deverão ser semelhantes à gestão de contas bancárias por parte dos bancos, inclusive permitindo trocas de *personal data agent* (tal como podemos trocar de banco) se o indivíduo assim o entender (World Economic Forum 2011).

Um local onde podemos criar um EDS é no sítio da Mydex[18]. Aqui, a EDS é designada como PDS (*Personal Data Store*). A PDS é cifrada com uma chave que fica na posse exclusiva do utilizador, não tendo a Mydex acesso a ela. A Mydex funciona como um infomediário (Hagel III & Rayport 1997), i.e., como uma plataforma que potencia os contactos e que intermedia as partilhas de dados do utilizador, em ambos os sentidos, com as várias entidades com quem ele os decidiu partilhar. Note-se que a intermediação para a partilha de um determinado dado não necessita de ter acesso ao conteúdo em claro desse dado. A Mydex apenas tem acesso aos itens de dados que o utilizador explicitamente tenha partilhado com ela.

Do ponto de vista funcional, um EDS pode ser organizado hierarquicamente em três camadas de serviços (Pfister & Schwabe 2013), como ilustra a Figura 7: (i) Serviços de Armazenamento na Nuvem, (ii) Serviços de Valor Acrescentado e (iii) Serviços de Integração de Processos.

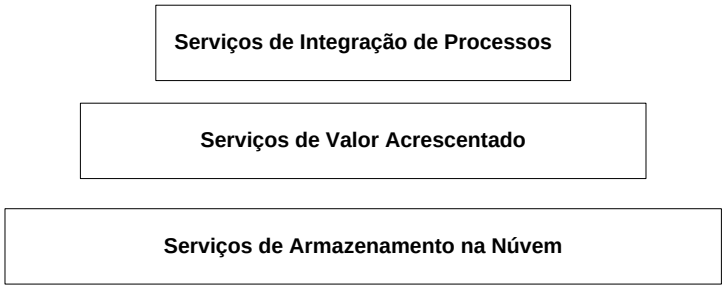

Figura 7: Camadas de serviços de um *Eletronic Data Safe* (Pfister & Schwabe 2013).

[18] https://mydex.org/

Na camada inferior localizam-se os serviços para armazenamento e segurança da informação. A camada de Serviços de Valor Acrescentado, que se baseia na camada inferior, disponibiliza serviços como (i) partilha de itens de informação, (ii) componentes de colaboração e (iii) geração de relatórios e de mineração de dados. A camada superior, serviços de integração de processos, cujos serviços se baseiam nos oferecidos pela camada de Serviços de Valor Acrescentado, pode ser usada para enviar e receber itens de informação para processos de negócio eletrónico e de governo eletrónico de várias organizações, não estando preso a nenhuma organização em particular.

Como os autores do modelo apresentado não apresentam endereços de exemplos reais de soluções que implementem serviços da camada de Serviços de Integração de Processos, ao contrário do que acontece em relação aos Serviços de Valor Acrescentado, deduzimos que não as terão encontrado. Na nossa análise ao *Personal Data Store* Mydex verificámos a menção à possibilidade da existência de serviços que se enquadram nas características apontadas para a camada Serviços de Integração de Processos. No entanto, eles estão previstos como serviços adicionais, prestados por aplicações de gestão de informação pessoal externas, operando sobre os dados do indivíduo disponibilizados pela Mydex sobre controlo do indivíduo (Mydex 2010). Algo semelhante acontece no modelo PDE, em que as funcionalidades de integração de processos não estão previstas para o EDS, mas sim para um outro componente do ecossistema, os serviços analíticos de dados (*Data Analytic Services*), não sendo dado nenhum exemplo concreto dessas funcionalidades (Cavoukian 2012; Cavoukian 2013). Por isso concluímos que a EDS é essencialmente uma plataforma para a partilha controlada dos dados do indivíduo.

Não obstante as vantagens que o conceito de PDE oferece, é necessário ter em consideração que ele lida com informação pessoal e por isso é necessário ter muita atenção aos detalhes. Segundo Cavoukian, "*nas mãos erradas, os EDS e as atividades dentro do PDE podem ser exploradas como uma significativa ferramenta de vigilância*" (Cavoukian 2012). Por essa razão é necessária uma atitude proactiva em relação à privacidade, nomeadamente é necessário incorporar a privacidade desde a conceção dos sistemas, *Privacy by Design* (PdB) (Cavoukian 2012; Cavoukian 2013). Outros problemas em iniciativas distribuídas são analisados em (Narayanan et al. 2012).

2.4.2 CARD SELECTORS

O Seletor de Cartões (*Card Selector*) é uma aplicação que representa a carteira do utilizador no designado *Information Card Model* (Burton 2009). O *Information Card Model* é um modelo de gestão de identidades, suportado pela *Information Card Foundation*[19], da qual fazem parte empresas como a Microsoft, Google, Oracle, entre outras. Este modelo baseia-se em *Information Cards* (IC), uma metáfora do cartão de apresentação que as pessoas transportam nas suas carteiras.

O Seletor de Cartões é uma aplicação do utilizador, o equivalente à sua carteira, onde ele transporta os seus cartões (*Information Cards*). Cada *Information Card* representa uma identidade do utilizador que é usada em determinado contexto, i.e., o utilizador pode ter um cartão que representa a sua identidade no relacionamento com o seu banco, outro que representa a sua identidade no relacionamento com a sua empresa, e outros que são identidades por si geridas para usar no acesso a sítios na Web que peçam a sua identificação. A Figura 8 apresenta um seletor de cartões, o entretanto descontinuado, *Windows CardSpace* da Microsoft com vários *Information Cards*.

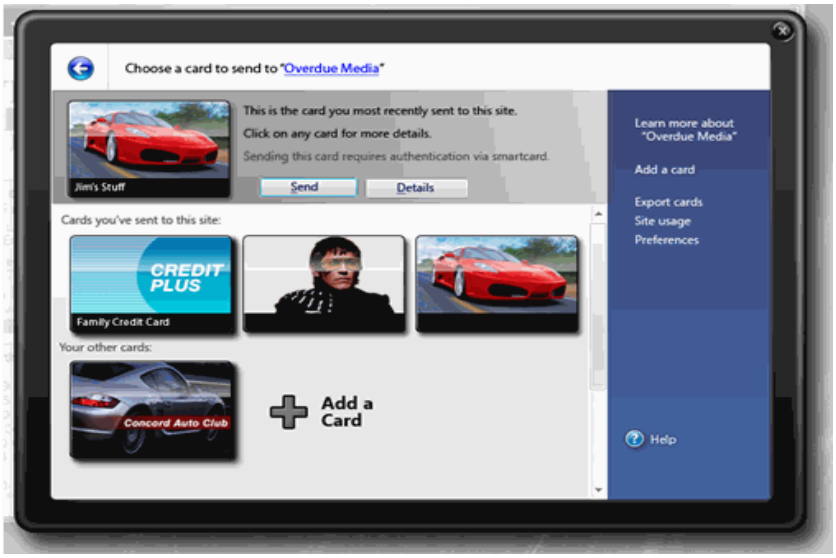

Figura 8: Information Cards no Windows CardSpace (Microsoft 2006)

No modelo de interação do *Information Card Model* participam três entidades: o (i) Fornecedor de Identidade (*Identity Provider,* IdP) que emite cartões (*managed cards*) e

[19] http://informationcard.net/

que, quando solicitado pelo utilizador, lhe fornece a informação de identidade para o identificar perante (ii) o *Relying Party* (RP), que é a entidade que necessita da identidade do utilizador para lhe prestar um qualquer serviço pretendido por este, e (iii) o Seletor de Cartões, aplicação onde o utilizador gere a sua identidade através dos seus cartões.

Os cartões podem ser de dois tipos: os *managed cards*, emitidos pelos IdP, e que correspondem a identidades geridas por entidades terceiras, e os cartões autoassinados (*self-signed cards*), que são cartões criados pelo próprio utilizador. Num exemplo de interação típica com *managed cards* (ver Figura 9), o utilizador acede a um RP (1) que lhe pede identificação (2), o Seletor de Cartões abre e o utilizador verifica que informação de identidade lhe está a ser pedida e escolhe o cartão que pretende utilizar para o identificar (3). O Seletor de Cartões contacta o correspondente IdP (4), que após adequada autenticação lhe envia a informação de identificação pedida (5). Após receber e eventualmente verificar a informação de identificação pedida (6), o Seletor de Cartões reenvia-a para o RP (7) que, após verificação e aceitação da informação de identidade, disponibiliza ao utilizador o serviço por este pretendido (8).

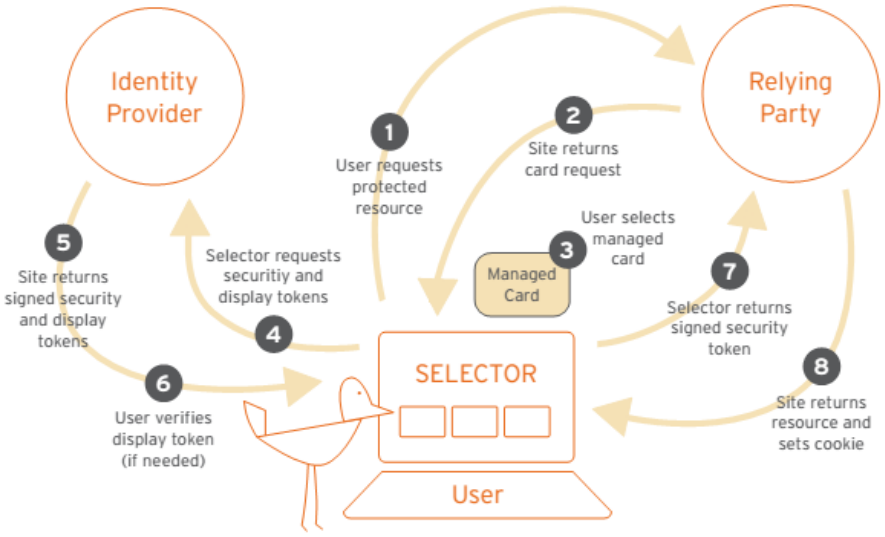

Figura 9: Interação genérica usando um *managed card* (Burton 2009).

A vantagem deste modelo de identificação é que coloca o utilizador no controlo do fluxo da sua identidade e torna esse fluxo transparente, uma vez que o utilizador controla que informação de identidade fornece e a quem (Burton 2009).

2.4.3 *MASHUPS*

Mashups (Merrill 2009) é uma tecnologia da designada Web 2.0 que permite ao utilizador o desenvolvimento rápido de aplicações que combinam recursos provenientes de várias fontes, de forma adaptada à situação ou ao interesse do utilizador. Os *mashups* são criados de forma bastante intuitiva, não sendo normalmente necessário que o utilizador tenha conhecimentos de programação. Um exemplo comum de utilização de *mashups* é a localização em mapas de dados que contenham informação de localização, o que permite uma melhor visualização e compreensão da informação contida nesses dados.

Do ponto de vista arquitetural, um *mashup* envolve três entidades: (i) os fornecedores de conteúdo/APIs, (ii) o servidor do *mashup* e (iii) o navegador (*browser*) do utilizador (Merrill 2009). Apesar dos *mashup* estarem albergados num servidor, podem ser executados no servidor ou no navegador do utilizador, ou partes em cada um deles.

O acesso aos recursos é feito através da captura em páginas Web (*scrapers*), ou através de APIs disponibilizadas pela entidade dona dos dados. As APIs são encapsuladas em componentes (*gadgets*) que podem ser utilizados em editores gráficos de *mashups*. A criação de *mashups* é feita de forma intuitiva através a colocação e remoção (*drag & drop*) de componentes no editor e do estabelecimento de ligações que definem o fluxo de dados entre componentes.

Os *mashups* podem tirar partido de SOA, uma vez que também se baseiam em componentes de software, e desta forma aproximar a SOA dos utilizadores finais (Soriano et al. 2008). Podem mesmos ser enriquecidos para interpretar informação semântica para facilitar a combinação de recursos (Li et al. 2011; Benhaddi et al. 2012; Bianchini et al. 2012). Assim, o paradigma SOA, que não foi concebido a pensar no utilizador final, mas sim nas interações entre organizações, beneficia ao ganhar uma interface que permite ao utilizador final criar *mashups* com base em serviços (encapsulados como componentes). Por este facto, os *mashups* podem mesmo ser usados na integração de sistemas de diferentes instituições (Siebeck & Wolfgang 2009). No entanto, a sua utilização em empresas é normalmente em integração de dados com sistemas externos, existindo vários obstáculos, organizacionais e técnicos, à sua utilização para compor processos de negócio (*business process mashups*) (Vrieze et al. 2009; Xie et al. 2010).

Os *mashups* são, assim, uma tecnologia promissora por, dada a sua flexibilidade e facilidade de utilização, permitir aos utilizadores finais desenvolver aplicações talhadas para os seus requisitos específicos. No entanto, além da já apontada dificuldade na criação

de *mashups* de processos, existem outras como a dificuldade de integração de mecanismos de autenticação quando os recursos estão protegidos por mecanismos de controlo de acessos (Hashimoto et al. 2009; Zarandioon et al. 2009) e questões de privacidade, devido à combinação de dados provenientes de várias fontes (Warner & Chun 2008; Barhamgi et al. 2011).

2.5 RESUMO

Neste capítulo começámos por fazer uma análise à prestação de serviços de governo eletrónico. Começámos pela prestação de serviços discreta, em que cada instituição presta os seus serviços de forma autónoma e independente das restantes instituições e avançámos até ao paradigma da prestação de serviços OEV, tendo sido realçada a sua faceta de serviço integrado (i.e., que incorpora serviços prestados por outras instituições) e a sua utilidade para o cidadão. Abordámos mais alguns aspetos como a composição de serviços e um modelo de serviços OEV que caracteriza os serviços parciais em três tipos. Podemos concluir desta análise que a prestação de serviços integrados implica o fluxo de dados do cidadão entre instituições e que esse fluxo de dados é controlado pelas instituições que controlam a prestação do serviço integrado, o que pode levantar receios quanto ao respeito da privacidade dos cidadãos, nomeadamente dúvidas sobre se o princípio da divulgação da menor informação necessária para a prestação dos serviços está a ser respeitado.

Abordámos também a interoperabilidade, condição necessária para a prestação de serviços envolvendo mais do que uma instituição, em que consideramos quatro níveis: técnico, sintático, semântico e organizacional, sendo que é a este último nível que ela é mais difícil de atingir devido a obstáculos sociais, políticos e legais, entre outros. A interoperabilidade refere-se apenas à colaboração entre instituições, o que significa que a interação do cidadão com a AP fica confinada ao acesso a um Portal que disponibiliza os serviços prestados pelas várias instituições, sejam eles serviços OEV ou não. Uma vez que os serviços OEV são serviços integrados, envolvendo várias instituições, o cidadão não tem um efetivo controlo sobre a disseminação da sua informação.

Abordámos o problema da confiança dos cidadãos que dificulta a adesão destes a muitas iniciativas de governo eletrónico. A confiança tem duas vertentes: a vertente da confiança na tecnologia e a vertente da confiança no Estado. Para ultrapassar a primeira, é necessário que as instituições mostrem competência nos mecanismos para a proteção da

comunicação e da informação do cidadão. Para a segunda vertente, é necessário que as instituições não se fiquem por declarações de boas práticas, mas que efetivamente demonstrem a sua implementação e a operação de acordo com elas, que implementem mecanismos que promovam a transparência.

Abordámos o conceito de dados pessoais, a gestão de identidades, e os vários conceitos associados a identidade, e o conceito de privacidade, que está intrinsecamente associado à proteção dos dados pessoais. Concluímos que a privacidade se refere ao controlo sobre os dados pessoais, que a divulgação de dados pessoais deve ser minimizada ao mínimo indispensável e que o Estado deve ter uma atitude exemplar em relação ao respeito pela privacidade dos cidadãos.

Fizemos uma breve apresentação de SOA, uma arquitetura baseada em serviços que preconiza uma modularização que suporta a integração de serviços, e a tecnologia de Web Services que suporta a sua implantação.

Por fim, analisámos três tipos de aplicações que se posicionam, ou podem posicionar, no centro da comunicação para a obtenção de serviços e no controlo da divulgação da informação do utilizador. São elas: o *Electronic Data Safe*, do paradigma *Personal Data Ecosystem*, o *Card Selector*, do paradigma *Information Card Ecosystem*, e *Mashups*, uma ferramenta da designada Web 2.0. Os dois primeiros tipos de aplicação inserem-se em iniciativas que promovem o controlo pelo individuo da sua informação pessoal, um objetivo comum ao modelo CHAPAS. Por diferentes razões, nenhuma delas permite a obtenção de serviços OEV, mas reconhecemos potencial ao EDS para permitir a sua obtenção, diretamente ou através de alguma aplicação associada que explore as funcionalidades de armazenamento e proteção de dados que ele disponibiliza. Quanto à tecnologia Mashups, tem um grande potencial para poder vir a permitir a composição de serviços OEV, mas de momento tal não é possível, sendo essencialmente utilizados para fazer a combinação de dados provenientes de diversas origens.

3 O MODELO CHAPAS

Neste capítulo apresentamos o modelo CHAPAS (*Citizen-side HAndling of Public Administration e-Services*) para a prestação ao cidadão de serviços OEV (serviços orientados a eventos da vida). Um serviço OEV é, do nosso ponto de vista, a obtenção coordenada de um conjunto de serviços prestados por diversas instituições, serviços parciais, que no seu conjunto satisfazem as necessidades relacionadas com um evento da vida do cidadão.

O modelo CHAPAS caracteriza-se por permitir ao cidadão a obtenção de serviços OEV, compostos por múltiplos serviços parciais, eventualmente prestados por múltiplas instituições, em que é o cidadão através do seu Chappie (*Citizen APPlication to Interact with E-services*), uma aplicação que corre em ambiente controlado pelo cidadão (e.g. o seu computador pessoal), que compõe e coordena a obtenção desses múltiplos serviços parciais.

Nesta apresentação começamos por definir os objetivos que se pretendem alcançar com o modelo CHAPAS, na secção 3.1, após o que apresentamos o modelo de prestação de serviços OEV, na secção 3.2, e a forma como é feita a composição e execução dos serviços OEV, na secção 3.3. Em seguida, analisamos, na secção 3.4, os padrões de interação da aplicação do utilizador, o Chappie, com as Instituições Prestadoras de Serviços (IPS) para a obtenção dos serviços que compõem um serviço OEV. Na secção 3.5 apresentamos o conceito de documento e de atributo no modelo CHAPAS. Na secção 3.6 apresentamos os mecanismos fornecidos pelo modelo CHAPAS para a minimização de informação do cidadão nos documentos que fluem entre instituições e na secção 3.7 apresentamos o mecanismo de agregação de documentos com base em atributos ofuscados, que permite uma maior minimização da informação do cidadão. De seguida, na secção 3.8, apresentamos a Política de Documentos Necessários (RDP – *Required Documents Policy*), o documento onde uma IPS disponibiliza toda a informação necessária

para que um seu serviço possa ser obtido pelo Chappie do Cidadão. Na secção 3.9, fazemos a discussão de um conjunto de aspetos relevantes do modelo CHAPAS e concluímos finalmente na secção 3.10.

3.1 OBJETIVOS

Como vimos, na secção 2.1.5, no modelo de prestação de serviços integrados a prestação de serviços OEV é feita sob o controlo de alguma instituição. Significa isso que essa instituição, que presta o serviço OEV, tem acesso a toda a informação que o cidadão disponibiliza para a obtenção do serviço, sendo ela a responsável pela difusão pelas restantes instituições da informação necessária para a obtenção de cada um dos vários serviços parciais que compõem o serviço OEV. Ou seja, o cidadão não tem um efetivo controlo sobre o fluxo da sua informação pelas várias instituições com que (indiretamente) interage para a obtenção do serviço OEV pretendido. Assim, um dos objetivos do modelo CHAPAS é colocar o cidadão no controlo da obtenção do serviço OEV, o que implica que o cidadão deve participar na composição do serviço OEV que pretende obter de forma a adequá-lo às suas circunstâncias e de forma a saber exatamente que instituições participam na sua prestação e que informação tem de disponibilizar a cada uma delas.

Apesar de ser importante para o cidadão o conhecimento de qual a informação que disponibiliza a cada instituição, isso não é suficiente porque subsiste a possibilidade de as instituições pedirem/receberem informação excessiva face ao serviço a que se destinam. Assim, um outro objetivo do modelo CHAPAS é fomentar a redução do fornecimento de informação do cidadão às instituições para o mínimo indispensável à prestação dos serviços por ele pretendidos.

3.2 MODELO DE PRESTAÇÃO DE SERVIÇOS

No modelo de prestação de serviços CHAPAS, ilustrado na Figura 10, participam dois atores fundamentais: o Cidadão, representado pela aplicação Chappie e serviços prestados ao cidadão por IPS, que podem ser múltiplas.

As IPS disponibilizam serviços (serviços parciais) que podem ser usados pelo Chappie para compor serviços OEV talhados para as circunstâncias e necessidades do cidadão. Pressupomos, para efeitos da prestação dos serviços ao cidadão, que as várias IPS não têm qualquer interação direta entre si, sendo toda a informação necessária à prestação de um serviço fornecida pelo cidadão na invocação do respetivo serviço. Ou seja, a prestação de serviços das IPS enquadra-se perfeitamente no modelo prestação de serviços dispersos (vide secção 2.1.3). Esta prestação de serviços deve, no entanto, ser feita de acordo com os princípios SOA, i.e., os serviços disponibilizados pelas IPS devem ter uma interface bem definida e devem ser autónomos (*loosely coupled*) e modulares, de forma a poderem ser usados pelo cidadão como componentes a usar na composição do seu serviço OEV, talhado para as suas circunstâncias específicas.

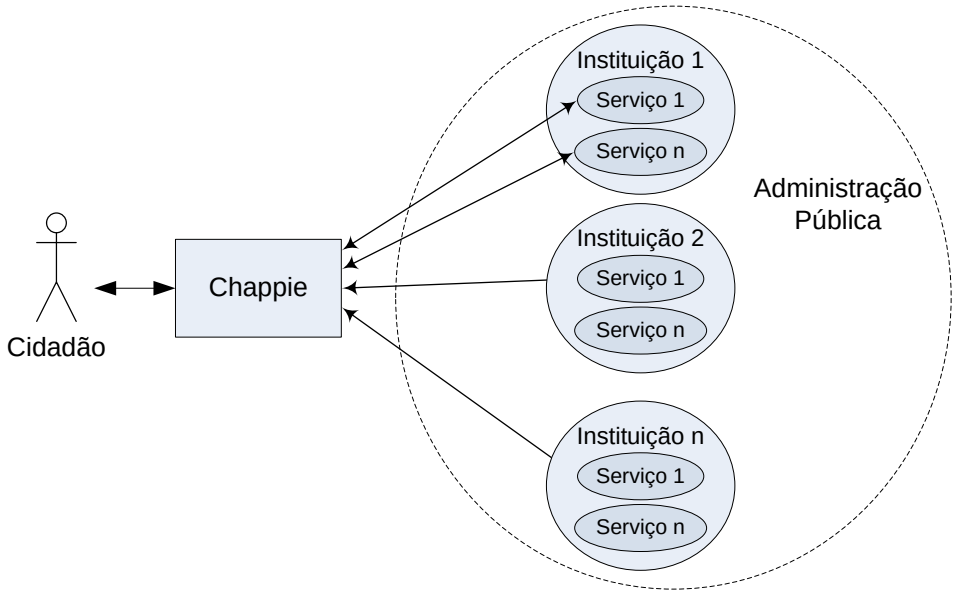

Figura 10: Visão alto nível do modelo CHAPAS para a implementação de serviços OEV.

A aplicação Chappie representa o cidadão na interação com as IPS. O Chappie é executado num dispositivo do cidadão e todo o seu funcionamento é controlado por este. A composição e execução (obtenção) de serviços OEV, que serão abordados em detalhe na secção 3.3, são feitas pelo cidadão no seu Chappie. Para auxiliar na composição dos serviços a obter, as IPS devem indicar, para cada um dos serviços que prestam, qual a informação que o cidadão tem de fornecer para o obter e qual a informação que o cidadão obtém como resultado final da prestação do serviço. Para cada serviço, esta indicação é disponibilizada num documento, a designada Política de Documentos Necessários (RDP - *Required Documents Policy*) (Gomes et al. 2012), que deve estar sempre publicamente acessível. A RDP será abordada em detalhe na secção 3.8.

Consideramos que o fluxo de informação é baseado em documentos, documentos estes que contêm um conjunto de atributos de uma ou mais entidades. O conceito de documento é abordado em detalhe na secção 3.5. Assim, para obter um determinado serviço, o cidadão poderá ter de disponibilizar um conjunto de informação, sob a forma de documentos, necessária para a prestação do serviço. Eventualmente terá de ir obter esses documentos a outras IPS, o que é feito através da obtenção de serviços nessas IPS. Como resultado de um serviço existe sempre a emissão de pelo menos um documento, que o cidadão deverá recolher (Overeem et al. 2007). Obviamente, como resultado de um serviço poderá haver a produção de resultados de outra natureza mas, do ponto de vista do modelo CHAPAS, apenas os documentos são relevantes.

Para obter um serviço OEV, o Chappie terá primeiro de determinar quais os serviços (serviços parciais, do ponto de vista do serviço OEV) que o compõe e apenas depois, se o cidadão assim o entender, poderá ir tratar da sua obtenção. A composição de serviços OEV no modelo CHAPAS é abordada na secção 3.3.

Depois de composto o serviço, o Chappie tem de interagir com as IPS para obter os serviços pretendidos pelo cidadão. Esta interação obedece a padrões que são abordados na secção 3.4.

3.3 Composição e execução de Serviços OEV

Um serviço OEV é composto por um conjunto de serviços (serviços parciais) que têm de ser obtidos na totalidade, de acordo com algum plano, para satisfazer o evento da vida do cidadão. Assim, antes de se poder executar um serviço OEV, é necessário compô-lo, i.e., selecionar um conjunto de serviços parciais e combiná-los, construir um plano de execução, de forma que se produza o resultado pretendido.

A composição de serviços OEV no modelo CHAPAS é semiautomática e realiza-se no Chappie. A composição não se baseia em predefinições de serviços OEV feitas por especialistas em AP e disponibilizadas em algum portal (vide secção 2.1.5.3), mas sim no pressuposto que uma IPS sabe quais os requisitos que coloca ao cidadão para a prestação de cada um dos seus serviços parciais. Nomeadamente, que sabe: (i) quais documentos o cidadão, dependendo das suas circunstâncias, deve fornecer, (ii) eventuais imposições sobre o conteúdo de cada documento exigido ao cidadão e (iii) (eventualmente) quais as instituições, e respetivos serviços, que emitem cada um os documentos exigidos ao

cidadão. Esta informação deve constar na já mencionada RDP que as IPS devem ter publicamente disponível para cada um dos seus serviços. A RDP é abordada em detalhe na secção 3.8.

Como se viu na secção 2.1.5.3, os serviços parciais de um serviço OEV podem ser classificados em três tipos (Todorovski et al. 2007): (i) Serviços Cruciais, cuja obtenção é fundamental; (ii) Serviços de Suporte, que produzem informação necessária para os serviços cruciais e cuja obtenção, ou não, depende das circunstâncias do cidadão, (iii) e Serviços Complementares, que são serviços opcionais que podem ser obtidos para complementar o serviço OEV. Além disso, analisando o modelo geral de referência para serviços OEV, apresentado na mesma secção, verificamos que se não considerarmos as exceções em que os serviços cruciais dependem de circunstâncias e se não considerarmos os serviços do tipo Complementares, os *workflows* genéricos de serviços OEV terminam sempre com um serviço parcial do tipo Serviço Crucial que tem obrigatoriamente ser obtido para que o evento de vida seja satisfeito, quaisquer que sejam as circunstâncias dos cidadãos, e que vamos designar como serviço Terminal. Verificamos também que todos os serviços parciais que precedem o serviço Terminal, quaisquer que sejam os seus tipos, emitem documentos dos quais ele, de forma direta ou indireta, depende (de forma direta quando emitem um documento por ele exigido e indireta quando emitem um documento que serve para obter outro ou outros serviços parciais que, esses sim, emitem documentos por ele exigidos).

Assim, se considerarmos que as IPS publicam uma RDP para cada um dos serviços por elas prestados, então, sabendo qual é o serviço Terminal, o Chappie pode dar início ao processo de composição do serviço OEV para identificar todos os restantes serviços que devem ser previamente obtidos e a ordem pela qual devem ser obtidos. Este processo começa com a análise da RDP do serviço Terminal, porventura complementada com informação adicional do cidadão, para determinar quais os documentos exigidos ao cidadão e quais os serviços parciais onde estes documentos podem ser obtidos. De seguida, o Chappie obtém as RDPs desses serviços parciais que também são analisadas para determinar que documentos são exigidos ao cidadão e quais os serviços onde podem ser obtidos, e assim sucessivamente. Desta forma, o Chappie constrói uma árvore de dependências, com raiz no Serviço Terminal e que agora também designamos como Serviço Raiz, que inclui todos os serviços parciais que devem ser obtidos para satisfazer o evento da vida do cidadão que representa. A Figura 11 ilustra esta árvore de dependências.

A árvore de dependências construída pelo Chappie não representa um serviço OEV genérico com o conjunto total dos serviços parciais que podem ter de ser obtidos pelo cidadão. Representa sim um serviço OEV talhado para as circunstâncias específicas de um cidadão em concreto, uma vez que o processo de composição da árvore de dependências é semiautomático, permitindo ao cidadão participar na sua composição, talhando-a à sua medida. O processo de composição não é automático por duas razões: (i) porque a necessidade de alguns documentos é condicionada por regras que são função de circunstâncias específicas do cidadão (e.g. se é menor de idade), pelo que é necessário que o cidadão as indique, e (ii) porque existem documentos que podem ser produzidos por serviços de várias IPS (e.g., um certificado de habilitações pode ser emitido por muitas escolas), pelo que o cidadão tem de indicar em concreto qual o serviço e instituição onde o documento deve ser obtido. Em relação a este último caso, não foi abordada neste trabalho a forma como o cidadão determina qual o serviço em concreto onde o documento deve ser obtido, mas poderá ser, por exemplo, através da consulta (com tecnologia semântica ou não) a um repositório de serviços ou através da utilização de *Information Cards*, que representam o relacionamento do cidadão com uma IPS e podem conter informação sobre os serviços por esta prestados, em que o cidadão apenas escolheria qual o *Information Card* a usar.

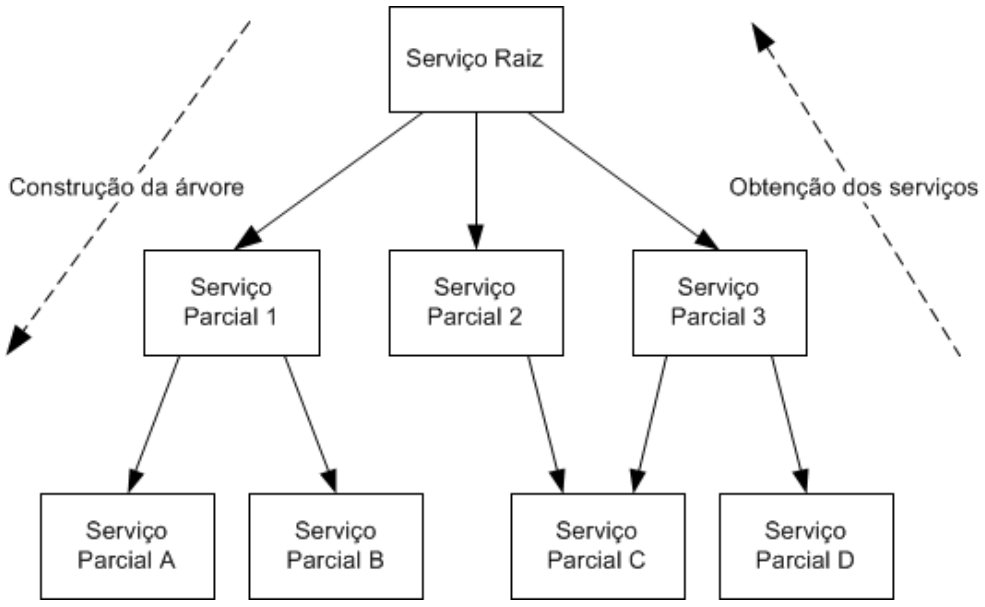

Figura 11: Árvore de dependências para a obtenção de um serviço OEV no CHAPAS.

Depois de construída a árvore de dependências pode dar-se início à obtenção do serviço OEV, caso o cidadão assim o entenda. Para isso o Chappie deve começar pela

obtenção dos serviços parciais nas folhas da árvore de dependências e progredir até atingir a raiz. Na Figura 11 está também indicada a direção da obtenção das RDPs, para a construção da árvore de dependências, e a direção da obtenção dos serviços para a satisfação do serviço OEV. A obtenção do serviço na raiz da árvore de dependências (Serviço Raiz) corresponde a completar o serviço OEV na sua totalidade.

Para uma melhor visualização das interações do Chappie com os vários serviços parciais que compõem um serviço OEV, apresentamos a Figura 12 que ilustra a sequência das interações do Chappie para a obtenção das RDPs e para a obtenção dos correspondentes serviços. Nele podemos ver que a interação com cada serviço é composta por três passos: 1) obtenção da RDP, 2) obtenção dos documentos para fornecer ao serviço e 3) obtenção do serviço. Podemos também observar que o passo 2) é por sua vez uma nova interação com um serviço e que se decompõe num mesmo conjunto de 3 passos. Note-se que a árvore de dependências apenas fica completa depois de ter sido executado o passo 1 com todos os serviços. A obtenção do serviço OEV é feita com a execução dos passos 2 e 3 para cada serviço, conforme os documentos vão sendo obtidos, terminando sempre no Serviço Raiz.

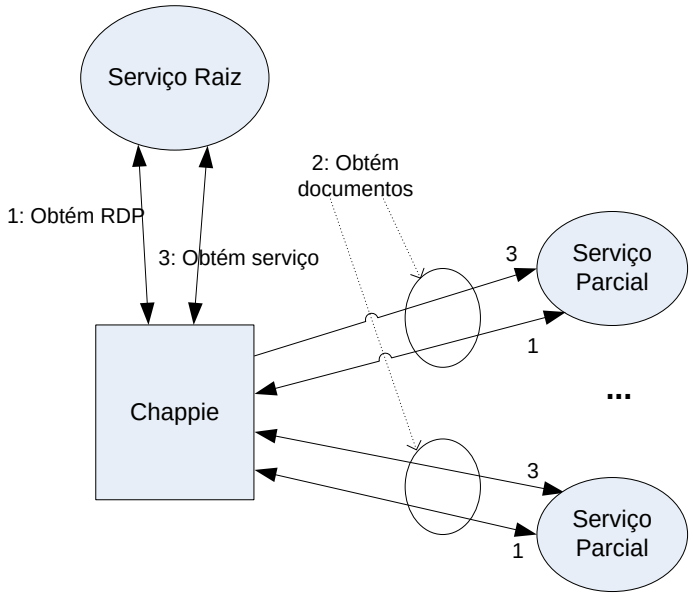

Figura 12: Sequencia das interações do Chappie para a obtenção das RDP e para a obtenção dos correspondentes serviços

3.4 PADRÕES DE INTERAÇÃO

Nesta secção vamos analisar os padrões de interação entre o Chappie e as IPS para a obtenção dos serviços. A comunicação no modelo CHAPAS é baseada em mensagens e os padrões de interação definem os tipos de mensagens que ocorrem numa interação entre duas entidades.

Como vimos na secção 2.3.2, as interações básicas com *Web Services* decorrem de acordo com quatro padrões de troca de mensagens: Pedido-Resposta, Sentido Único, Solicitação-Resposta e Notificação. Analisando a adequação ao modelo CHAPAS de cada um dos padrões de troca de mensagens de *Web Services*, de forma isolada, verificamos que o padrão de Pedido-Resposta pode ser considerado o padrão de interação básico para prestação de serviços no modelo CHAPAS. De acordo com este padrão, um cidadão que pretende obter um determinado serviço, faz o pedido desse serviço ao respetivo IPS, através do seu Chappie, enviando toda a documentação necessária, e de imediato recebe uma resposta contendo todos os documentos produzidos como resultado da execução do serviço. Apesar de este padrão de interação se poder aplicar à obtenção de alguns serviços no modelo CHAPAS, a maioria das interações é mais complexa, com padrões de interação que abordamos nas secções 3.4.1 e 3.4.2.

Na aplicação do padrão Solicitação-Resposta a uma interação do modelo CHAPAS, uma IPS tomaria a iniciativa de enviar uma mensagem para o Chappie e este enviaria uma mensagem de resposta. Este tipo de interação não faz muito sentido no contexto da prestação de serviços, uma vez que é a IPS que toma a iniciativa de solicitar algo ao cidadão, o que nos parece de alguma forma uma inversão do próprio conceito da prestação de serviço. É de notar também um aspeto importante que é a necessidade de o serviço ter de conhecer o endereço para onde enviar as solicitações ao cidadão, o que implica a ocorrência de uma prévia interação por iniciativa do cidadão para o fornecimento desse endereço. Ou seja, este padrão de interação apenas faz sentido quando, de alguma forma, associado a outros para produzir novos padrões de interação mais complexos, como veremos na secção 3.4.2. O prévio fornecimento de um endereço do cidadão pode ser uma aspeto crítico na prestação de serviços e será também analisado mais à frente, na secção 3.4.1.

Quanto ao padrão Sentido Único (*one-way*), o envio de uma mensagem sem direito a resposta, do Chappie para uma IPS, também não faz muito sentido na prestação de serviços do modelo CHAPAS, porque consideramos que o cidadão deve ter sempre uma

resposta em todas as interações com as IPS. Já no sentido oposto, o padrão Notificação, o envio de uma mensagem de uma IPS para o Chappie pode fazer sentido como veículo de notificação ao cidadão de eventos na sua relação com a IPS. Por exemplo, a sua utilização pode ser interessante para informar o cidadão de novidades sobre algum serviço, mas nunca poderá ser usado para notificações de maior responsabilidade porque estas carecem de uma confirmação de receção por parte do cidadão. Além disso, tal como acontece com o padrão Solicitação-Resposta, continua a subsistir o problema do prévio conhecimento do endereço do cidadão para onde deveriam ser enviadas as notificações.

Nas secções seguintes analisamos a necessidade de padrões de interação mais complexos para satisfazer os requisitos de comunicação do Chappie com as IPS para a obtenção de serviços.

3.4.1 INTERAÇÕES ASSÍNCRONAS

Na apresentação do padrão de interação Pedido-Resposta atrás realizada considerou-se que a resposta ao pedido chegava de imediato. Trata-se, por isso de uma interação síncrona, em que quem faz o pedido espera pela chegada da resposta que chega de imediato.

Existem, no entanto, situações em que a resposta a um pedido não é imediata, podendo demorar um intervalo de tempo mais ou menos longo e porventura irregular. Estas situações prefiguram interações assíncronas. As razões para uma interação ser assíncrona podem ser as mais variadas, sendo uma delas a existência de operações que têm de ser realizadas por um humano.

As interações síncronas são as mais simples e cómodas de lidar, uma vez que a satisfação dos pedidos é imediata. Só que implicam a total automatização do processamento dos serviços, o que nem sempre é possível. O problema com as interações assíncronas é que não se sabe quando chega a resposta aos pedidos. Isto tem impacto no cliente porque ele tem de decidir se fica à espera até que a resposta chegue, como faz nas interações síncronas, ou não. Enquanto a espera numa interação síncrona não é problemática, uma vez que a resposta chega de imediato, o mesmo não acontece nas interações assíncronas. Ficar à espera de uma resposta assíncrona implica o cliente ficar bloqueado, sem fazer mais nada, até que a resposta chegue, o que não é uma boa decisão tanto a nível da interface com o utilizador como a nível de gestão de recursos.

Existem dois tipos de abordagens às interações assíncronas, que passam pelo desdobramento da interação pedido-resposta em duas outras interações: (i) o cliente fica responsável por periodicamente ir inquirir se a resposta já está pronta (*polling*) e (ii) o cliente fornece um endereço para onde a resposta deverá ser enviada quando estiver pronta (*callback*).

Na abordagem por *callback*, ilustrada na Figura 13, o cliente faz o pedido do serviço, no qual indica um endereço para onde a resposta deverá ser enviada quando estiver pronta, e recebe uma confirmação (síncrona) da realização do pedido. Depois de realizar o pedido, o cliente não fica à espera da resposta. O servidor, quando a resposta ao pedido estiver pronta, irá enviar a resposta para o endereço fornecido pelo cliente.

No modelo CHAPAS a abordagem por *callback* não poderá ser usada se a comunicação entre o Chappie e o fornecedor de serviços for implementada exclusivamente sobre o protocolo HTTP. Em primeiro lugar, porque raramente os cidadãos possuem um endereço permanente para as suas máquinas. Note-se que os computadores pessoais normalmente não possuem nenhum nome DNS (*Domain Name System*), normalmente apenas máquinas servidoras possuem nomes DNS, e raramente possuem endereços IP públicos estáticos, seja porque normalmente os fornecedores de acesso à Internet usam endereços IP dinâmicos, ou por razões de mobilidade do cidadão entre redes. Em segundo lugar porque os computadores pessoais estão normalmente equipados com *firewalls* que bloqueiam comunicações iniciadas a partir do exterior. Como o fornecedor de serviços toma a iniciativa de enviar a resposta quando ela estiver disponível, significa que para uma *firewall* de um computador pessoal se trata de uma comunicação com origem externa que, por essa razão, será bloqueada, impedindo a sua receção pelo Chappie.

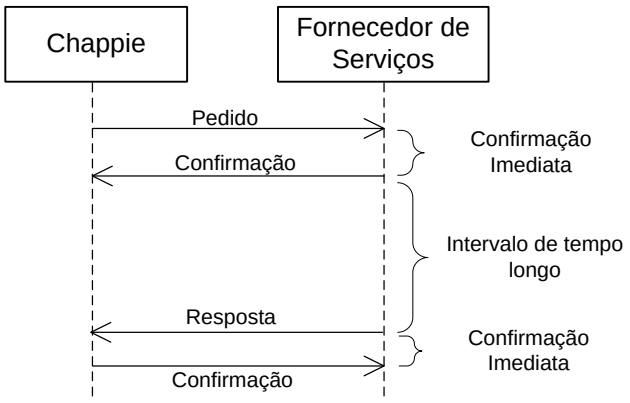

Figura 13: A interação Pedido-Resposta assíncrona implementada através da abordagem por *callback*.

No entanto, a abordagem *callback* poderá ser usada no modelo CHAPAS se implementada usando correio eletrónico (SMTP) para o envio da resposta. A resposta será enviada para a conta de correio eletrónico, num servidor de correio eletrónico, onde ficará armazenada até que o Chappie a obtenha. Note-se que neste caso já não existem os problemas atrás indicados, uma vez que um endereço de correio eletrónico é um endereço público e estático que pode perfeitamente ser usado para o envio de comunicações para o cidadão e não existem comunicações bloqueadas pela *firewall*, uma vez que a caixa de correio não está residente na máquina do cidadão mas sim num servidor publicamente acessível para o envio de mensagens. No entanto, implica uma maior complexidade nas aplicações dos fornecedores de serviços e no Chappie, uma vez que terão de lidar com um segundo protocolo de comunicações.

Por sua vez, a abordagem *polling*, ilustrada na Figura 14, implica o desdobramento de uma interação Pedido-Resposta assíncrona em duas interações Pedido-Resposta síncronas. Na primeira interação faz-se o pedido de forma normal, mas a resposta será uma confirmação do pedido que deverá incluir um código que o Chappie deverá usar para posteriormente inquirir se a resposta está pronta. A segunda interação, que poderá ser executada múltiplas vezes até que finalmente se obtenha o resultado do processamento do serviço, envolve um inquérito para verificar se a resposta já está pronta, que deve incluir o código fornecido na resposta da primeira interação, e uma resposta que poderá conter o resultado do serviço solicitado, caso em que ele já foi processado, ou poderá conter uma indicação de que o serviço ainda não foi processado.

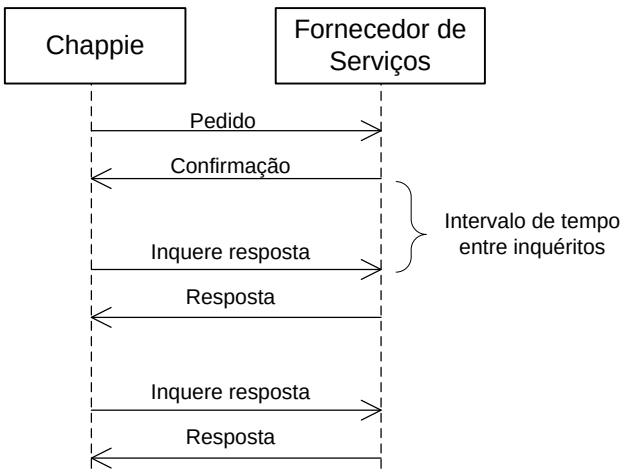

Figura 14: A interação Pedido-Resposta assíncrona implementada através da abordagem por *polling*.

No modelo CHAPAS, a adoção da abordagem *polling* não é problemática para o Chappie, mas poderá acarretar uma sobrecarga do lado dos IPS se muitos clientes (Chappies) fizerem *polling* em simultâneo.

3.4.2 INTERAÇÃO PEDIDO-RESPOSTA COM SOLICITAÇÃO ADICIONAL

Um outro tipo de situações em que o padrão de interação Pedido-Resposta básico não é adequado, acontece quando não é possível fornecer no pedido de um serviço toda a informação necessária para a prestação deste. Um exemplo desta situação acontece quando um serviço não tem um preço fixo, sendo o seu valor calculado após a avaliação do pedido. Nesta situação, a resposta da IPS será uma solicitação de documentos adicionais (por exemplo, o comprovativo do pagamento do serviço, a obter numa instituição bancária), que o Chappie deverá ir obter para depois fornecer como resposta à solicitação adicional. Note-se que neste padrão de interação a mensagem de solicitação adicional pode conter documentos, que poderão ser usados para a obter o(s) documento(s) solicitados. A Figura 15 ilustra este padrão de interação.

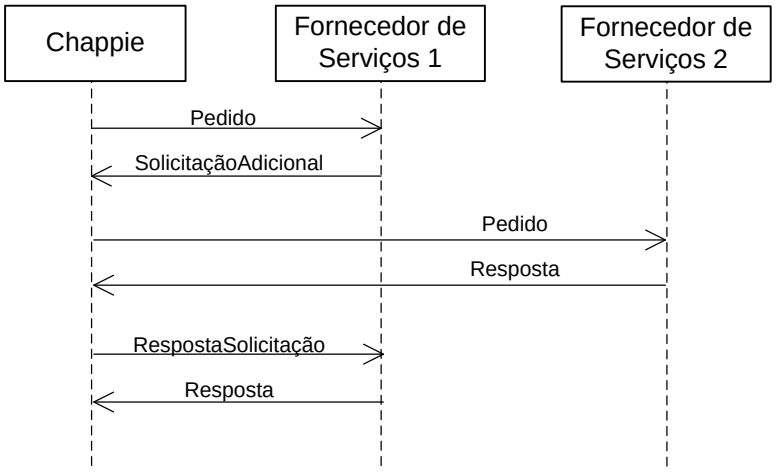

Figura 15: A interação Pedido-Resposta com solicitação adicional.

Este padrão de interação deverá ser bastante comum na prestação de serviços se considerarmos que muitos serviços necessitam de um pagamento que deve ser feito na altura da obtenção do serviço. Note-se que mesmo nas situações em que se trate de um serviço de preço fixo, é normal que as pessoas não se sintam confortáveis em fazer o

pagamento do serviço antes de fazer o seu pedido, pelo que mesmo nestas situações este padrão de interação pode ser o mais adequado.

É de notar ainda que nesta interação Pedido-Resposta com solicitação adicional, tanto a mensagem de solicitação adicional com a resposta final podem também ser assíncronas, o que introduz mais alguma complexidade a este padrão de interação.

3.5 CONCEITOS DE DOCUMENTO E DE ATRIBUTO

O documento é o elemento básico de comunicação entre instituições na arquitetura CHAPAS. Ele veicula informação sobre cidadãos ou sobre alguma outra entidade ou assunto, normalmente relacionada com o cidadão em causa, de uma IPS emissora do documento para outra(s) IPS(s) recetora(s)/consumidora(s) do documento.

Consideramos um documento como um conjunto de dados num formato digital estruturado (por exemplo baseado em XML). Neste sentido, uma imagem digitalizada de um documento em papel não se considera como um documento. No entanto, nada obsta a que essa mesma imagem digitalizada possa estar contida dentro de um documento. A razão pela qual os documentos devem ser estruturados é para permitir ao Chappie e às IPS aceder ao seu conteúdo através de indicações fornecidas pelas IPS (usando XPath, por exemplo).

Os documentos referem-se a entidades, sejam elas físicas (como pessoas, carros, etc.) ou virtuais (como processos, assuntos, etc.), podendo um documento referir-se a mais do que uma entidade. Consideramos que o conteúdo de um documento, os dados que veicula, consiste num conjunto de atributos das entidades a que o documento se refere. Alguns destes atributos poderão ser atributos identificadores das respetivas entidades a que pertencem, i.e., podem permitir a identificação das entidades a que se referem.

Uma chamada de atenção para a linguagem usada neste documento. Para facilitar, vamos frequentemente utilizar expressões como “os documentos contêm atributos” ou “os atributos num documento”. Deve-se ter em atenção que os atributos referidos nestas expressões não são atributos do documento, mas sim os atributos das entidades a que os documentos se referem, que estão contidos no documento, e que constituem os dados veiculados pelo documento. Além disso, a utilização do termo atributo nunca se refere a atributos de elementos XML, a menos que tal seja explicitamente indicado.

De um ponto de vista mais técnico, ou de mais baixo nível, um documento é uma estrutura de dados, em formato digital, que obedece a um determinado esquema (*schema*). Este esquema deve ser público para garantir que todas as partes interessadas possam aceder ao seu conteúdo.

O número de potenciais documentos envolvidos nos múltiplos serviços OEV que um cidadão pode obter é muito grande, o que implica que o número de potenciais esquemas de documentos seja também muito grande. Além disso, os esquemas dos documentos podem variar ao longo do tempo. Por isso, o Chappie é agnóstico em relação aos documentos, i.e., não sabe interpretar nem atribuir qualquer semântica ao conteúdo dos documentos.

É importante referir que os esquemas dos documentos trocados entre as instituições são definidos pelas próprias instituições que os emitem/consomem ou por alguma entidade de normalização. O modelo CHAPAS não define o esquema de qualquer documento trocado entre instituições.

Para que uma instituição possa confiar no conteúdo de um documento que recebe, é necessário que (i) confie na instituição emissora do documento, i.e., que lhe reconheça competência em relação ao assunto objeto do documento, e (ii) que o documento contenha uma assinatura digital válida que comprove a autenticidade do documento. Por exemplo, para que uma instituição confie num certificado de habilitações referente a uma licenciatura do ensino superior, é necessário que reconheça a competência da instituição emissora para produzir o certificado de habilitações (poderá reconhecer se for emitido por uma instituição de ensino superior, mas com certeza não reconhecerá se for emitido por uma instituição que se dedique a uma outra qualquer atividade) e que o certificado de habilitações esteja assinado digitalmente pela instituição de ensino superior que o produziu. A forma como é estabelecida a confiança entre as instituições não é assunto deste trabalho.

3.6 MINIMIZAÇÃO DA INFORMAÇÃO

Como vimos no capítulo anterior, a divulgação de informação excessiva sobre um cidadão, principalmente de dados pessoais, acarreta riscos para a sua privacidade. Mas as instituições também correm riscos ao obter e armazenar informação excessiva sobre os cidadãos. Em primeiro lugar porque tal pode levar à perda de confiança dos cidadãos na

instituição, caso se gere nos cidadãos um sentimento de que há um abuso de poder por parte da instituição. Em segundo lugar porque, caso a informação na posse da instituição seja ilicitamente apropriada por terceiros, pode haver lugar a responsabilização criminal, isto para além da já mencionada perda de confiança dos cidadãos na instituição. É de notar que quanto mais informação uma instituição guarda, mais apetecível ela se torna como alvo para a ataques com vista à obtenção ilícita dessa informação. Ou seja, ambas as partes, instituições e cidadãos, têm interesse na minimização da informação a pedir ao cidadão.

A divulgação excessiva de informação do cidadão pode ocorrer em duas situações: (i) quando, para a prestação de um serviço, uma IPS pede mais informação do que a estritamente necessária e (ii) quando a informação produzida por um serviço é excessiva em relação à sua finalidade. Um exemplo bastante frequente desta segunda situação ocorre quando o cidadão tem de apresentar recibos de serviços como o fornecimento de água ou de luz como comprovativos de residência, em que claramente a informação sobre o consumo efetuado é excessiva.

A minimização da informação a fornecer pelo cidadão não é possível sem a participação das IPS, uma vez que são elas que determinam qual a informação necessária para a prestação de cada um dos seus serviços. Assim, as IPS devem ser sensibilizadas para apenas pedirem ao cidadão documentos que contenham informação estritamente necessária para a prestação dos seus serviços. No entanto, isto pode não ser suficiente porque subsiste a segunda situação indicada no parágrafo anterior, que pode fazer com que uma instituição receba documentos contendo informação excessiva em conjunto com informação necessária, mesmo que não a pretenda receber.

Assim, no modelo CHAPAS as IPS podem especificar, nas RDP dos seus serviços, para cada documento que pedem ao cidadão, quais os atributos que efetivamente pretendem receber, devendo os restantes ser omitidos do documento. No entanto, esta omissão de atributos de um documento apenas pode ser realizada pela IPS que o emite, uma vez que a sua realização por qualquer outra entidade provoca o invalidar da assinatura digital do documento. Por isso, as IPS devem suportar a possibilidade de os pedidos de serviços poderem especificar, para cada documento a emitir, qual o conjunto de atributos cujos valores devem ser incluídos no documento, devendo os restantes ser omitidos, ou vice-versa.

3.7 AGREGAÇÃO DE DOCUMENTOS BASEADA EM ATRIBUTOS OFUSCADOS

Quando um cidadão pretende obter um determinado serviço de uma IPS, é comum ser obrigado a entregar vários documentos, possivelmente provenientes de diferentes origens, cada um contendo um conjunto de informação (atributos) referentes ao cidadão e/ou a outras entidades (coisas materiais ou imateriais) relacionadas com o serviço solicitado. Para permitir a correta identificação das entidades a que um documento se refere e para permitir a agregação de vários documentos de uma mesma entidade (i.e., associá-los a uma mesma entidade), é natural a inclusão em cada documento de um conjunto mais ou menos alargado de atributos de identidade das entidades a que o documento se refere. Como exemplo de atributos de identidade frequentemente utilizados para este efeito, para o caso de cidadãos, temos o nome, o número de identificação civil, o número de identificação fiscal, a morada, nomes de pais, etc. A agregação de um conjunto de documentos a uma determinada entidade implica verificar se os atributos de identidade contidos nesses documentos se referem ou não à entidade em causa, i.e., verificar se o valor de cada um desses atributos é o mesmo nos vários documentos a agregar.

Os atributos de identidade de um cidadão são dados pessoais, logo sensíveis do ponto de vista da privacidade, pelo que a sua divulgação deve ser cuidadosa. Assim, um documento não deverá conter mais atributos de identidade do que aqueles necessários para a identificação das entidades no contexto a que o documento se destina (Cameron 2005). Mais, como regra geral, deve-se seguir o princípio da não divulgação de mais informação do que a estritamente necessária para o fim pretendido.

Existem, aliás, situações em que nem sequer é desejável a revelação dos atributos de identidade do cidadão, ou de outra entidade, a que um documento se refere mas, em simultâneo, é necessário agregar esse documento com outros documentos. Trata-se de situações em que há atributos (de identidade) que apenas são necessários para a agregação de documentos, não sendo necessários para qualquer outro fim, em termos da prestação do serviço. Ou seja, são situações em que se podem usar pseudónimos. Um exemplo bem ilustrativo desta situação ocorre num hipotético cenário de consulta médica anónima de segunda opinião através da Internet, em que o paciente não pretende revelar a sua identidade. Neste cenário, os atributos de identidade presentes nos vários documentos (exames médicos) que o paciente entrega não devem ser revelados, uma vez que

permitiriam revelar a identidade deste. No entanto, para garantir a validade do diagnóstico, a clínica médica pretende ter a garantia de que todos esses documentos se referem a um mesmo paciente, o que implica ter uma forma de verificar que a identidade do paciente é a mesma em todos os documentos, sem com isso revelar a verdadeira identidade deste. Para este tipo de situações propomos a agregação de documentos com base em atributos ofuscados (Gomes et al. 2011).

Tal como acontece na agregação normal, a agregação com base em atributos ofuscados depende da comparação dos valores de atributos de identidade nos vários documentos a agregar, só que agora estes estão ofuscados. Para que se possa comparar os valores ofuscados de um determinado atributo presentes em vários documentos, sem os revelar, e daí concluir que se trata de um mesmo valor em claro, é necessário que o atributo em causa tenha um mesmo valor ofuscado em todos esses documentos. Por exemplo, se uma agregação de vários documentos se basear no atributo Número de Utente do Serviço Nacional de Saúde (NSNS), então o valor ofuscado deste atributo tem de ser o mesmo em todos os documentos a agregar. No fundo, os valores ofuscados funcionam como pseudónimos do cidadão, um pseudónimo por cada atributo, devendo o cidadão usar os mesmos pseudónimos nos diferentes documentos que pretende agregar.

Como já foi referido, no modelo CHAPAS são as instituições que especificam, nas RDP dos serviços que prestam, qual a informação externa (documentos) que o cidadão deve fornecer para obter o correspondente serviço. Esta especificação deve identificar quais os documentos que devem ser fornecidos e, para cada um deles, quais os atributos, referentes ao assunto objeto do documento, cujos valores devem obrigatoriamente constar no documento. Uma vez que são também as instituições que sabem como vão agregar os vários documentos que recebem do cidadão, o que inclui saber quais os atributos que vão ser comparados e se estes atributos são necessários para alguma outra finalidade para além da agregação, a especificação dos documentos a apresentar pelo cidadão deve ser complementada com a indicação de quais os atributos que vão ser usados na agregação de documentos e que devem apresentar os seus valores ofuscados.

Para facilitar a linguagem, a partir deste momento vamos designar os atributos usados para a agregação de documentos como atributos de agregação.

3.7.1 OFUSCAÇÃO DE ATRIBUTOS

A ofuscação de um valor é realizada pela aplicação de uma transformação de ofuscação sobre esse valor. Para poderem servir o objetivo da agregação com valores ofuscados, as transformações de ofuscação devem satisfazer as seguintes propriedades:

- Devem ser configuráveis por um conjunto de parâmetros de ofuscação.
- Devem produzir valores ofuscados dependentes unicamente dos respetivos valores em claro e dos parâmetros de ofuscação utilizados.
- Devem produzir valores ofuscados a partir dos quais não seja fácil (seja virtualmente impossível) determinar quais os correspondentes valores em claro, a não ser que se conheçam os parâmetros de ofuscação usados.

A primeira propriedade permite que ao usarmos diferentes conjuntos de parâmetros de ofuscação se obtenham diferentes valores ofuscados para um mesmo valor em claro. Isto é importante para impedir a agregação de documentos referentes a uma determinada entidade (i.e., em que há atributos de agregação com o mesmo valor, em claro), mas que tenham sido emitidos em contextos diferentes e que não se pretende que sejam relacionáveis.

A segunda propriedade é importante para garantir que múltiplas ofuscações de um mesmo valor de um atributo, utilizando os mesmos parâmetros de ofuscação, produzem sempre um mesmo valor ofuscado, o que é fundamental para se poder fazer agregação com base em atributos ofuscados.

A terceira propriedade é importante para garantir a confidencialidade dos atributos ofuscados. Determina que a revelação dos atributos ofuscados fica dependente do conhecimento dos parâmetros de ofuscação utilizados, o que permite ao cidadão o controlo sobre a revelação dos atributos ofuscados, assumindo que não há conluio entre a instituição que ofuscou os atributos e alguma das instituições que recebem os atributos ofuscados.

Tendo em conta os critérios atrás enunciados, as funções de ofuscação podem ser funções criptográficas das seguintes tipos:

- Cifras simétricas por blocos;

- Assinaturas digitais:

    a) Usando cifra assimétrica (com restrições);

    b) Usando códigos de autenticação de mensagens (funções MAC - *Message Authentication Codes*).

Associados a cada um dos tipos de funções criptográficas acima mencionados existe um conjunto de parâmetros, indicados na Tabela 1, cujos valores têm de ser fornecidos para que a respetiva função possa ser utilizada para ofuscar o valor de um atributo. Designamos como parâmetros de ofuscação ao conjunto algoritmo de ofuscação e respetivos parâmetros de configuração.

Note-se que a tabela inclui um outro parâmetro que é a Codificação. Este parâmetro indica qual a codificação usada para incluir o valor ofuscado no documento. Repare-se que os valores ofuscados são valores em binário e, portanto, não podem ser incluídos dessa forma em documentos de texto. Por isso, é necessária uma codificação para transformar os valores binários em texto. Um exemplo de codificação comum é a Base64 (Josefsson 2006).

Cifra simétrica	Assinatura Digital com criptografia assimétrica	Assinatura Digital com funções MAC
Algoritmo	Algoritmo	Algoritmo
Chave	Chave "privada"	Chave
Algoritmo de *padding*	Algoritmo de *padding*	---
Modo de cifra	---	---
Vetor inicial (dependendo do modo de cifra)	---	---
Codificação	Codificação	Codificação

Tabela 1: Funções de ofuscação e respetivos parâmetros de configuração.

Dependendo do tipo de função de ofuscação usado, a natureza do valor ofuscado vai ser diferente. Se a função de ofuscação for do tipo cifra simétrica, o valor ofuscado produzido será um criptograma, que pode posteriormente ser decifrado para obter o valor original. No entanto, se a função de ofuscação for do tipo assinatura digital, seja usando

cifra assimétrica ou funções MAC, o valor ofuscado produzido será uma assinatura, que não possui função inversa, o que impede a obtenção do valor original a partir da assinatura.

Assim, quando se utiliza ofuscação por assinaturas digitais, a revelação de um valor original apenas pode ser feita recalculando o valor ofuscado, i.e., verificando se o valor ofuscado (assinatura) foi de facto obtido aplicando um determinado conjunto de parâmetros de ofuscação sobre um determinado valor original. Já a revelação do valor de um atributo que tenha sido ofuscado utilizando cifras simétricas, além de poder ser realizada utilizando o processo atrás indicado para as assinaturas digitais, pode também ser realizada com uma operação de decifra que usa apenas os parâmetros de ofuscação e os valores ofuscados.

Os algoritmos de assinatura digital com cifra assimétrica podem não satisfazer o segundo critério definido para as funções de ofuscação. Isto acontece porque podem introduzir um valor aleatório no processo de *padding*, usado durante a operação de assinatura, precisamente para impedir que um determinado valor em claro produza sempre um mesmo valor de assinatura (e.g. *Probabilistic Signature Scheme* (Jonsson & Kaliski 2003)). No entanto, essa randomização de assinaturas não é crítica (Jonsson & Kaliski 2003), podendo ser eliminada em casos onde seja uma contrariedade. Assim, para poderem ser usados na ofuscação de atributos, os algoritmos de assinatura digital com cifras assimétricas têm de ser parametrizados para não utilizarem *padding* com valores aleatórios (e.g. PKCS #1 V1.5) ou, caso usem *padding* (e.g. PSS), para usarem como *padding* um determinado valor "aleatório" fornecido como parâmetro.

Na Tabela 1 é indicado que a assinatura deverá ser realizada com uma chave "privada". A razão por que se usa aspas para designar o tipo de chave usada é porque normalmente as assinaturas são realizadas com a componente privada de um par assimétrico mas, neste caso, essa assunção tem um sentido diferente. Com efeito, se considerarmos que se usa pares assimétricos RSA, se dois ou mais serviços ofuscarem um atributo com a mesma componente privada do mesmo par RSA, ela deixa naturalmente de ser privada. Porém, a chave "privada" usada na ofuscação não deverá ser revelada a terceiros, i.e., a entidades não envolvidas na ofuscação, para evitar que outros possam descobrir, através de técnicas elementares de pesquisa exaustiva (em domínios de pesquisa limitados), o atributo assinado. Note-se que a assinatura poderá ser realizada com as componentes pública ou privada de um par RSA, mas que, em qualquer caso, a

chave assimétrica usada por um agente ofuscador deverá sempre permanecer secreta, caso contrário poder-se-á facilitar a descoberta do atributo ofuscado.

Um aspeto que pode ser importante na seleção da função criptográfica a usar na ofuscação é a dimensão do valor ofuscado produzido. Com efeito, a maioria dos tipos de funções criptográficas indicados gera valores ofuscados com um tamanho diferente do tamanho dos correspondentes valores em claro. Por exemplo, o tamanho dos criptogramas produzidos pela cifra por blocos (cifra simétrica ou assimétrica) é sempre um múltiplo do tamanho do bloco característico do algoritmo de cifra usado (número de bits que o algoritmo impõe para os dados a cifrar), o que implica que o tamanho dos criptogramas é sempre maior ou igual do que o tamanho do correspondente texto em claro. Outro exemplo, quando se usam assinaturas (criptografia assimétrica ou funções MAC), o tamanho a assinatura produzida é constante e independente da dimensão do texto em claro a que corresponde.

Esta variação do tamanho do valor ofuscado com o algoritmo usado na ofuscação, e a sua diferença em relação ao tamanho do correspondente valor em claro, pode eventualmente ser um problema para a entidade que recebe os documentos com os atributos ofuscados. Por exemplo, pode ser um problema para o armazenamento dos atributos ofuscados numa base de dados, uma vez que não se sabe à partida o tamanho que cada um dos atributos ofuscados terá. Por isso, poderá ser interessante considerar para funções de ofuscação apenas cifras contínuas (ou cifras por blocos em modos de cifra contínuos: e.g., OFB, CFB, CTR) ou a cifra FNR (*Flexible Naor and Reingold*) (Dara & Fluhrer 2014), que permitem ter criptogramas com o tamanho do correspondente valor em claro.

3.7.2 CONTROLO DA OFUSCAÇÃO

Para que o valor ofuscado de um atributo seja o mesmo nos vários documentos em que está presente, é necessário que duas condições sejam satisfeitas: (i) que o valor em claro do atributo a ofuscar seja o mesmo para os vários documentos e (ii) que a ofuscação do valor do atributo, em cada um dos vários documentos, seja realizada utilizando os mesmos parâmetros de ofuscação.

A primeira condição implica que haja um prévio acordo quanto aos formatos de dados, para garantir que um atributo é descrito da mesma forma em todos os documentos a agregar (interoperabilidade sintática), e um cuidado redobrado com a sincronização dos valores dos atributos conhecidos por múltiplas instituições. A título de exemplo, quanto ao

formato dos dados, considerando o nome de um cidadão, este não pode ser uma sequência de N caracteres num documento (e.g., "Hélder Gomes") e noutro documento ser decomposto em duas sequências de caracteres, uma com o primeiro nome (e.g., Hélder) e outra com o último nome (e.g., Gomes). Quanto à sincronização dos valores, trata-se de evitar a existência de diferentes valores para um mesmo atributo, como o nome do cidadão escrito de forma diferente (e.g, "Hélder" e "Helder"), por exemplo.

A segunda condição tem a ver com o controlo da ofuscação e uma conclusão imediata que se extrai dela é que a escolha da ofuscação a usar (i.e., a escolha das funções de ofuscação, e dos respetivos parâmetros de configuração) não pode ser feita individualmente por cada instituição que emite documentos com atributos de agregação ofuscados, porque desta forma seriam usados diferentes parâmetros de ofuscação.

Note-se também, que a definição do material criptográfico (chaves, vetores iniciais, etc.), que faz parte dos parâmetros de ofuscação, não deve ser feita pela instituição que pede os documentos com os atributos com valores ofuscados (e que define quais os atributos cujos valores devem ser ofuscados). Isto porque quem tem conhecimento desse material criptográfico fica com informação que facilita, ou mesmo permite, fazer a correspondente revelação, algo que não se pretende que possa ser feito pela instituição que irá receber os valores ofuscados, uma vez que o objetivo é exatamente impedir o seu acesso aos valores reais dos atributos. No entanto, a instituição que vai receber os documentos com os valores ofuscados deve poder definir qual o algoritmo de ofuscação e a codificação a usar para cada atributo para poder ter controlo sobre o tamanho dos valores ofuscados, o que implica a definição prévia de um conjunto de algoritmos (incluindo modos de cifra e *padding*) a suportar obrigatoriamente por todas as IPS.

Um outro ponto importante é que as instituições devem assinar digitalmente os documentos que emitem, para que os recetores dos documentos (seja o cidadão sejam outras instituições) possam verificar e confiar na origem e autenticidade dos documentos recebidos. A inclusão de uma assinatura digital num documento protege a integridade do documento, i.e., qualquer alteração a um documento realizada posteriormente à inclusão de uma assinatura digital, invalida essa assinatura digital. Isto implica que a realização da assinatura digital de um documento que contenha atributos com valores ofuscados tenha de ser feita posteriormente à ofuscação desses valores, ou seja, implica que seja a própria instituição que emite um documento com atributos com valores ofuscados a proceder à respetiva ofuscação dos valores desses atributos.

Assim, como a definição dos valores dos parâmetros de ofuscação não pode ser feita pelas instituições que produzem os documentos com os atributos a ofuscar, nem pelas instituições que os vão receber, apenas o cidadão, através do seu Chappie, o pode fazer. Mais, é do interesse do próprio cidadão fazer essa definição porque isso permite-lhe verificar a correção dos valores ofuscados, o que é fundamental para a confiança na ofuscação, e para eventualmente revelá-los a terceiros, sempre que tal seja pertinente.

Assim, uma das funções do Chappie será a gestão da ofuscação de atributos em documentos. Esta gestão consiste essencialmente: (i) na definição das funções de ofuscação a usar, para cada atributo a ofuscar (caso a instituição que pretende os documentos não o tenha feito); (ii) na definição dos valores para os parâmetros de ofuscação, como por exemplo a definição das chaves e vetores iniciais; (iii) na comunicação dos parâmetros de ofuscação às IPS que vão emitir os documentos com atributos ofuscados (i.e., que vão fazer a ofuscação), ao fazer os pedidos dos correspondentes serviços; (iv) no armazenamento dos atributos de ofuscação para eventual posterior reutilização e/ou para permitir uma posterior revelação dos valores reais dos atributos ofuscados; e (v) na verificação da veracidade dos atributos ofuscados.

Ter em atenção que para ser possível a revelação e a verificação seletiva dos valores dos atributos ofuscados, o controlo da ofuscação deve ser baseado no atributo e não no documento, tal como proposto por (Lopes & Shin 2007). Isto implica a definição de um conjunto de parâmetros de ofuscação por cada atributo a ofuscar.

No entanto, como um atributo de agregação está presente em múltiplos documentos, para que o seu valor ofuscado seja o mesmo em todos esses documentos, ele tem de ser produzido usando os mesmos parâmetros de ofuscação. Como o Chappie é agnóstico em relação ao conteúdo dos documentos, isto implica que a especificação, numa RDP, dos atributos a ofuscar seja feita de uma forma transversal aos vários documentos a agregar, i.e., de forma a identificar esse atributo em cada um dos documentos onde está presente. Por exemplo, no cenário da consulta médica anónima de segunda opinião, se a agregação dos exames médicos for baseada no atributo número de utente do Serviço Nacional de Saúde (NSNS), este deve ser especificado de forma que o Chappie saiba identificar o atributo com o NSNS em todos os exames e demais documentos apresentados pelo paciente, qualquer que seja o nome que ele tenha nesses documentos.

A verificação da veracidade dos valores dos atributos ofuscados é um aspeto importante para fomentar a confiança do cidadão no processo de ofuscação. Uma vez que o cidadão está na posse de toda a informação necessária para a revelação de todos os

atributos ofuscados, uma forma de fazer a verificação é através da apresentação num ecrã dos correspondentes valores em claro, após a prévia revelação dos valores ofuscados. Apesar de esta forma de validação dos valores ofuscados ser a mais fidedigna, depender exclusivamente dela poderá ser incómodo para o cidadão, uma vez que poderá haver situações com um grande número de documentos a verificar. Além disso, ela não é possível para todos os tipos de funções de ofuscação, nomeadamente não é possível para as ofuscações realizadas utilizando assinaturas digitais. Assim, para permitir a verificação automatizada dos atributos ofuscados, as instituições devem emitir duas versões de cada documento: uma versão com os atributos ofuscados e uma outra versão com todos os atributos com os seus valores em claro. Esta última poderá ser usada como referência para a validação automática dos valores ofuscados por parte do Chappie. Para impedir uma segunda utilização desta versão do documento com os valores dos atributos em claro, ela não deverá ser assinada digitalmente pela entidade emissora, mas deverá ser enviada em mensagem assinada, em conjunto com a versão ofuscada, para garantir a sua autenticidade e integridade.

Em relação à comunicação dos parâmetros de ofuscação às IPS que vão proceder à ofuscação, ela deve ser efetuada no pedido do serviço que produz o documento a ofuscar e obviamente deve ser feita de forma confidencial para impedir o acesso ilegítimo por parte de terceiros.

3.8 Política de Documentos Necessários (RDP)

A Política de Documentos Necessários (*Required Documents Policy*, RDP) de um serviço é um documento público onde, de uma forma detalhada, uma IPS define os seus requisitos em relação a um serviço por ela prestado. Uma IPS deve disponibilizar uma RDP para cada um dos serviços que presta.

Considera-se que um serviço produz sempre pelo menos um documento como resultado da sua execução. Exemplos de documentos a entregar a, ou produzidos por, um serviço são os recibos, as certidões, as declarações, etc. Obviamente que o resultado principal de um serviço pode ser outro que não a produção de documentos. No entanto, do ponto de vista do modelo CHAPAS apenas são relevantes os resultados que se manifestam sob a forma de documentos a obter pelo cidadão.

De forma genérica, uma RDP deve definir tudo o que seja relevante para obtenção do serviço, tal como: (i) os requisitos relativos aos documentos que o cidadão deve fornecer para obter o serviço; (ii) as características dos documentos produzidos como resultado da prestação do serviço; (iii) a especificação de dados relevantes para a prestação do serviço, que não estejam incluídos em nenhum documento, e que por isso tenham de ser introduzidos pelo cidadão; e (iv) a definição de circunstâncias dos cidadãos que sejam relevantes para a determinação de quais os documentos a entregar ou a obter por um cidadão em concreto.

Nas secções seguintes vamos abordar estes conteúdos da RDP.

3.8.1 ESPECIFICAÇÃO DOS DOCUMENTOS

Uma RDP especifica os documentos de entrada para o respetivo serviço (i.e., aqueles que o cidadão tem de fornecer) e os documentos que o serviço produz como resultado da sua prestação (i.e., aqueles que o cidadão obtém no final da execução do serviço). Relativo a qualquer documento, a RDP deve informar o cidadão sobre o propósito do documento, o seu conteúdo e outras eventuais informações de apoio ao cidadão.

A identificação de qualquer documento na RDP deve ser feita através de identificadores para consumo humano, que obviamente devem ser únicos no contexto da RDP, que o Chappie irá usar para mostrar ao cidadão que documentos são pedidos pelo serviço, e também através de identificadores que sirvam para identificar o documento por parte das entidades que o vão produzir, que podem ser, por exemplo, URIs (*Universal Resourse Identifiers*). A semântica associada a estes URIs pode ser qualquer uma e não é do conhecimento do Chappie, uma vez que se pretende que ele seja agnóstico em relação aos documentos.

A especificação dos documentos de entrada deve ainda incluir a identificação das IPS das quais o cidadão poderá ir obter os documentos pedidos, caso esta informação esteja disponível, e também especificar quais os atributos que devem obrigatoriamente constar em cada documento e indicar quais deles irão ser usados para a agregação dos documentos e, se for caso disso, quais destes devem ser ofuscados. Estes aspetos são abordados nas subsecções seguintes.

3.8.1.1 Atributos num documento

Como já foi referido, um documento contém atributos de uma ou mais entidades, relevantes para uma determinada finalidade. Por vezes, os documentos pedidos ao cidadão contêm mais informação do que a estritamente necessária para o objetivo pretendido. Para permitir a minimização da informação nos documentos pedidos ao cidadão, uma RDP deve, para cada documento, identificar os atributos que nele deve obrigatoriamente constar e, destes, quais devem constar de forma ofuscada. Na produção do documento, a IPS apenas deve incluir os atributos que forem indicados como devendo estar presentes, e omitir os restantes.

A identificação dos atributos deve ser feita de forma que o cidadão os possa reconhecer. Assim, eles devem ser identificados de forma única no contexto da RDP e com nomes e descrições sugestivas para o cidadão. Além disso, uma vez que o Chappie é agnóstico em relação aos documentos, os atributos devem também ser descritos de forma que o Chappie possa aceder ao seu conteúdo, para o apresentar ao cidadão ou para o validar. Para este efeito, no caso de documentos XML, a especificação de um atributo pode conter uma expressão XPath, por exemplo.

Os atributos devem também ser identificados de forma que as IPS que vão produzir os documentos também os possam identificar, o que pode também ser feito através de URIs ou também através de expressões XPath.

Os atributos de agregação são atributos identificadores que estão presentes em vários documentos e que identificam entidades a quem os documentos se referem. Para possibilitar a agregação com base em atributos ofuscados é fundamental que um atributo de agregação tenha o mesmo valor ofuscado em todos os documentos a agregar em que esteja presente, o que implica que tenha de ser ofuscado usando os mesmos parâmetros de ofuscação em todos esses documentos, qualquer que sejam as IPS que os emitam. Para isso, é necessário que o Chappie reconheça esse atributo nos vários documentos a agregar, de forma a poder enviar os mesmos parâmetros de ofuscação a todas as IPS que os vão emitir. No entanto, como cada documento tem o seu próprio esquema, isso permite que um mesmo atributo seja identificado de forma diferente em cada documento, o que impede que o Chappie reconheça que se trata do mesmo atributo, uma vez que é agnóstico em relação aos documentos. Assim, a RDP do serviço que pretende fazer a agregação com base em atributos ofuscados deve identificar estes atributos de agregação de forma transversal aos vários documentos em que estejam presentes.

Quando a agregação de documentos é feita com base em atributos de agregação com os seus valores em claro, não é obrigatória a identificação transversal dos atributos de agregação, uma vez que não é necessário gerir parâmetros de ofuscação. No entanto, dada a sensibilidade das operações de agregação, é aconselhável também fazer a identificação transversal dos atributos de agregação, para que o cidadão fique com um melhor conhecimento do uso que será dado à informação que fornece.

3.8.1.2 Emissores dos documentos

Assume-se que um documento apenas pode ser produzido pelo cidadão ou por uma instituição. Neste último caso, um documento pode ser produzido (i) por qualquer instituição, como acontece com uma fatura ou com os dados para realizar um pagamento, (ii) apenas por instituições de um determinado setor ou de um conjunto de setores, como acontece como os certificados de habilitações que apenas podem ser emitidos por instituições de ensino, (iii) ou por apenas alguma(s) instituição(ões) bem conhecida(s), como acontece com uma Caderneta Predial, que apenas é emitida pelas Finanças.

Para facilitar a obtenção dos documentos que um cidadão tem de fornecer a uma IPS para poder obter um determinado serviço por esta prestado, a respetiva RDP deve incluir, para cada um dos documentos que o cidadão tem de fornecer, uma caracterização de como o documento pode ser obtido, se tal for possível, devendo contemplar as várias possibilidades descritas no parágrafo anterior. Nos casos em que é bem conhecida a instituição que produz um documento, a RDP deve incluir o endereço onde o Chappie pode obter o serviço que emite o documento.

Nos casos em que o documento pode ser produzido por várias instituições, cabe ao cidadão indicar em concreto qual a IPS e respetivo serviço onde o documento pode ser obtido. A forma como o cidadão determina qual a IPS onde o documento deve ser obtido, e obtém o respetivo endereço do serviço onde o Chappie deve obter o documento, não foi objeto de estudo, mas apresentam-se duas possibilidades: uma é a existência de serviços de diretoria, tipo páginas amarelas, com listas de instituições/serviços habilitados a emitir cada tipo de documento e outra é a utilização de *Information Cards* (Burton 2009), cada um representando uma instituição com o qual o cidadão possui alguma forma de relacionamento, contendo os endereços dos serviços prestados pela respetiva instituição.

3.8.2 CIRCUNSTÂNCIAS DO CIDADÃO

Para alguns serviços, o conjunto de documentos que o cidadão tem de fornecer varia em função de circunstâncias do cidadão (Todorovski et al. 2006). Por exemplo, para a realização da escritura de compra de uma casa, o registo provisório de hipoteca apenas é necessário se se tratar de uma aquisição com recurso ao crédito. As RDP destes serviços devem caracterizar as circunstâncias do cidadão relevantes para a prestação do serviço, incluindo informação para auxiliar o cidadão na indicação da sua situação concreta (o que inclui informação que permita ao Chappie conduzir o diálogo com o cidadão para que este indique as suas circunstâncias, tal como o texto a apresentar e eventuais repostas possíveis), e um conjunto de regras, em função das circunstâncias, cuja avaliação determina quais os documentos, do total de documentos passíveis de ser pedidos, que um cidadão em concreto precisa de entregar para obter o serviço.

Note-se que o Chappie poderá conhecer algumas circunstâncias do cidadão (e.g., a nacionalidade) e, nesse caso, poderá avaliar a necessidade de entrega de documentos baseada nessas circunstâncias evitando questionar o cidadão. No entanto, tal obriga à utilização de alguma ontologia da AP que defina essas circunstâncias do cidadão e que seja utilizada pelas IPS no modelo Chapas.

3.8.3 INTRODUÇÃO DE DADOS

Existem casos em que os eventuais documentos fornecidos pelo cidadão não contêm todos os dados necessários para a prestação do serviço, sendo necessário a introdução de dados adicionais diretamente pelo cidadão. Por exemplo, para ir obter uma certidão de teor numa Conservatória de Registo Predial, o cidadão apenas necessita de identificar o prédio, não sendo necessário apresentar qualquer documento.

Nestes casos, a RDP deve especificar todos os dados que o cidadão deve introduzir. A especificação dos dados a introduzir, além de incluir informação para que o cidadão saiba que dados se pretendem e qual o objetivo do seu fornecimento, deve incluir elementos para o diálogo do Chappie com o cidadão com vista a possibilitar a introdução desses dados. Tal como referido para as circunstâncias do cidadão, o Chappie poderá possuir, armazenados, os valores de alguns destes dados comuns, mas tal implica a adesão do modelo CHAPAS a alguma ontologia da AP aceite pelas várias instituições participantes.

3.9 DISCUSSÃO

Depois de feita a apresentação do modelo CHAPAS, nesta secção vamos discutir alguns aspetos importantes do modelo e os seus impactos para o cidadão e para a AP.

3.9.1 COMPOSIÇÃO DE SERVIÇOS OEV

Como vimos na apresentação do paradigma de prestação dos serviços OEV no modelo CHAPAS (secção 3.2), nenhuma instituição possui uma visão completa da composição destes serviços. Cada instituição apenas sabe de si própria, isto é, sabe que documentos pede ao cidadão para que o mesmo possa obter os serviços por si prestados, mas não sabe o que é necessário para que o cidadão obtenha serviços de outras instituições. Cabe ao Chappie, com base nas indicações dos documentos pedidos por cada serviço, compor o serviço OEV pretendido pelo cidadão, i.e., construir a correspondente árvore de dependências talhada de acordo com as circunstâncias específicas do cidadão. Esta abordagem tem vantagens e desvantagens que vamos agora discutir.

A grande vantagem é a flexibilidade que permite na composição do serviço. Esta flexibilidade manifesta-se em dois aspetos: (i) na facilidade de incorporação de alterações em serviços (e.g., alterações nos documentos pedidos ao cidadão) e (ii) na facilidade de incorporação de serviços cuja instituição fornecedora não é conhecida à partida.

Numa implementação tradicional baseada em *workflows*, a alteração dos documentos pedidos ao cidadão (e.g. passar a ser necessário mais um documento) implica o desenho de um novo *workflow* para o serviço e a sua instalação (*deployment*) nos sistemas das instituições responsáveis pela sua prestação. No CHAPAS essa alteração não tem o menor impacto, uma vez que a árvore de dependências do serviço OEV é sempre composta na hora, pelo Chappie, com base nos documentos que as RDP dos serviços pretendidos pelo cidadão especificam como sendo de entrega obrigatória por parte do cidadão. Basta por isso alterar a RDP do serviço, para que as alterações sejam de imediato aplicadas na prestação de serviços.

A existência de situações em que múltiplas instituições podem fornecer um determinado documento necessário para a prestação de um serviço dificulta a definição do *workflow* global dos serviços OEV em que esse documento seja necessário. Isto porque poderá eventualmente haver diferentes requisitos para a sua obtenção, dependendo da instituição prestadora do serviço que emite esse documento. Nestes casos compete ao

cidadão identificar a instituição em concreto, e o respetivo serviço, que deve fornecer o documento e, em face dessa informação, o Chappie irá contactá-la para obter a respetiva RDP e continuar a construção da árvore de dependências do serviço OEV.

A identificação por parte do cidadão dos serviços em concreto a usar nestas situações é algo que não foi abordado neste trabalho e que reconhecemos que pode criar alguma dificuldade. Tal como mencionado na secção 3.8.1.2, parecem-nos possíveis duas soluções para este problema: através da existência de serviços de diretoria que poderiam ser consultados para a descoberta do serviço pretendido, ou através da utilização de cartões de apresentação (*Information Cards*) das instituições, semelhantes aos cartões de apresentação em papel, onde uma instituição além da sua identificação incluiria os endereços onde poderiam ser obtidos os seus serviços. Esta segunda possibilidade é do nosso agrado porque não envolve mais instituições e porque de alguma forma mapeia o relacionamento normal do cidadão com as instituições, isto é, quando existem várias instituições que prestam um determinado serviço, normalmente escolhe-se aquela com a qual já se tem algum tipo de relacionamento.

A desvantagem da abordagem do modelo CHAPAS para a composição dos serviços OEV é que a melhoria/otimização destes serviços, por exemplo para reduzir custos ou detetar eventuais serviços supérfluos, fica muito mais facilitada se houver uma visão global dos serviços OEV. Mais do que isso, se houver uma instituição que coordene a obtenção do serviço OEV, esta terá poder para influenciar as restantes instituições no sentido da implementação das eventuais melhorias.

No entanto, note-se que o modelo CHAPAS não impede que exista alguma instituição que tutele a prestação de serviços OEV e que mantenha e estude as árvores de dependências para a obtenção desses serviços. O que o modelo CHAPAS preconiza é que a obtenção dos serviços OEV deve ser feita diretamente pelo cidadão (i.e., sem a intermediação de nenhuma instituição), o que impede a existência de uma instituição com algum poder natural para negociar eventuais melhorias aos processos destes serviços (obviamente, excluindo o poder emanado de algum órgão político). Aliás, a análise dos serviços OEV também é importante para o próprio modelo CHAPAS no sentido de favorecer a oferta de serviços OEV ao cidadão. Repare-se que a prestação de serviços OEV no modelo CHAPAS implica a publicitação dos serviços Raiz de cada serviço OEV nalgum portal OEV passivo, para que eles possam ser fornecidos ao Chappie para este dar inicio a todo o processo de construção da árvore de dependências para a subsequente obtenção dos correspondentes serviços. Ora a descoberta dos serviços Raiz implica a análise dos

processos dos serviços OEV, pelo que pelo menos a instituição responsável pelo portal de disponibilização de serviços OEV deve fazer essa análise global.

3.9.2 *INTEROPERABILIDADE*

A interoperabilidade é um aspeto fulcral em qualquer iniciativa de governo eletrónico que envolva alguma forma de comunicação/colaboração entre instituições. Como vimos na secção 2.1.6, a interoperabilidade pode ser analisada em vários níveis: físico, sintático, semântico e organizacional. Nos parágrafos que se seguem vamos analisar o impacto do modelo CHAPAS em cada um dos referidos níveis de interoperabilidade.

A tecnologia que nos parece mais adequada para a implementação do modelo CHAPAS é a tecnologia de *Web Services*. Esta tecnologia usa essencialmente normas abertas e de larga aceitação, pelo que a sua utilização permite um grande nível de interoperabilidade. No entanto, o modelo CHAPAS implica a utilização de aplicações específicas, nomeadamente ao nível das IPS, que devem disponibilizar *WebServices* que funcionem de acordo com o paradigma de funcionamento do modelo CHAPAS, e ao nível do cidadão, que precisa de uma aplicação específica, o Chappie.

É nos níveis sintático e semântico que podem surgir os maiores problemas de interoperabilidade. Propositadamente considerou-se o Chappie como agnóstico em relação à comunicação entre instituições, precisamente para minimizar esse problema. Assim, o Chappie não assume nada em relação aos documentos que vai obter e fornecer às várias IPS, dependendo de informação das IPS para lidar com eles (e.g., para navegar nos documentos, para identificar os atributos de agregação, etc.). Desta forma, transforma a interoperabilidade nos níveis sintático e semântico essencialmente num problema entre instituições. No entanto, a interoperabilidade a estes níveis não é um problema exclusivo do modelo CHAPAS, mas sim um problema existente em qualquer outra iniciativa que vise a comunicação entre instituições.

O desenvolvimento de um modelo canónico de dados e de uma ontologia ao nível da AP e a sua adoção pela generalidade das IPS pode contribuir para minimizar o problema da interoperabilidade sintática e semântica, não apenas para o modelo CHAPAS como também para outras iniciativas de colaboração entre instituições. No entanto, para o caso concreto do modelo CHAPAS, teria a vantagem de permitir ao Chappie interpretar os dados contidos nos documentos e dessa forma poder prestar um melhor serviço ao cidadão.

Quanto à interoperabilidade ao nível organizacional, ela é grandemente simplificada no modelo CHAPAS porque este não coloca nenhum requisito especial em relação ao alinhamento da prestação de serviços com vista à integração em serviços mais complexos. No modelo CHAPAS, as instituições podem continuar a prestar os serviços tal como prestavam, apenas adaptando as suas interfaces para interagir com o Chappie. No entanto, o modelo CHAPAS não impede que existam reformulações de serviços com o objetivo de prestar serviços aos cidadãos mais simples e até mais eficientes, desde que não violem o princípio da não comunicação entre instituições para fins da prestação de serviços ao cidadão. Assim, no modelo CHAPAS, possibilita-se o fornecimento de serviços OEV sem necessidade de reorganizações internas das instituições, evitando-se os típicos conflitos e problemas ao nível organizacional e de poder que as reorganizações sempre levantam.

3.9.3 REORGANIZAÇÃO DA AP

Como vimos na secção 2.1.5, a integração da AP, necessária para a prestação de serviços OEV integrados, implica a reorganização das várias instituições no sentido de integrar processos de forma a criar um único processo simples e eficaz, por cada serviço OEV. Esta integração exige um forte alinhamento de processos e um alinhamento de objetivos entre instituições (interoperabilidade organizacional), o que gera imensos obstáculos à sua implementação, tais como obstáculos de índole política, organizacional, social, etc. (Hellman 2010). Por exemplo, levantam-se questões de poder sobre qual a instituição que vai controlar os novos processos, sobre a posse dos dados partilhados, etc. Por este motivo muitas destas iniciativas resultam em fracassos, o que é preocupante devido aos elevados custos envolvidos nas reorganizações de processos.

Por outro lado, como também vimos na secção 2.1.5, a prestação de serviços OEV coordenados tem muito menor impacto em termos da organização interna das instituições. Neste modelo, as várias instituições continuam a prestar os seus serviços sem alterações significativas, sendo a prestação do serviço OEV feita por uma outra instituição, normalmente a instituição que controla o portal onde o serviço OEV é disponibilizado ao cidadão. Apesar da vantagem deste modelo de prestação de serviços coordenados não implicar reorganizações nas instituições, ele é visto por (Vintar et al. 2002) como uma solução de curto prazo, porque este considera a integração total deve ser o objetivo principal a alcançar pela AP. No entanto, devido aos obstáculos à interoperabilidade organizacional e também devido às questões sobre a confiança do cidadão na integração

da AP, apresentadas em 2.1.7, e à necessidade de fomento da privacidade e confiança dos cidadãos na prestação dos serviços do estado, discutidas na secção 3.9.4, consideramos que a coordenação de serviços deve ser encarada como uma base válida para a prestação de serviços OEV. Assim, baseámos também o modelo CHAPAS na coordenação de serviços, mas colocando o controlo sobre a composição e a coordenação da obtenção dos serviços do lado do cidadão, mais propriamente no seu Chappie.

Por se basear na coordenação de serviços, também o modelo CHAPAS não impõe uma reestruturação significativa das instituições como condição para a prestação de serviços OEV. Apenas requer que as instituições adaptem a prestação dos serviços que tradicionalmente prestam para poderem interagir como o Chappie. Isto é uma vantagem comparativa porque não envolve custos significativos. No entanto, de modo nenhum se impede que as instituições possam ir sofrendo restruturações mais ou menos significativas no sentido de ir melhorando os seus processos internos, que eventualmente podem até ser pertinentes e desejáveis para melhorar a prestação de serviços de acordo com o modelo CHAPAS.

3.9.4 PRIVACIDADE E CONFIANÇA

O modelo CHAPAS permite ao cidadão a obtenção de serviços OEV, compostos por serviços parciais prestados por várias instituições, mantendo o cidadão no controlo do fluxo de informação entre as instituições, necessário para a prestação de cada um dos serviços parciais, e fomentando a minimização do fluxo de informação ao mínimo indispensável para a prestação de cada serviço parcial.

O cidadão controla o fluxo de informação entre instituições porque é a sua aplicação Chappie, executada numa plataforma controlada pelo cidadão (o seu computador pessoal, por exemplo), que compõe e obtém o serviço OEV. As instituições não precisam de dialogar diretamente entre si, para efeitos da prestação de serviços ao cidadão, uma vez que o cidadão fornece toda a informação necessária para a prestação do serviço pretendido, ainda que isso implique obter essa informação a partir de outras instituições. Uma vez que toda a informação agora passa pelo cidadão, ele tem o poder de a observar e registar, o que lhe permite avaliar se está, ou não, a fornecer informação excessiva a alguma instituição.

Este controlo sobre o fluxo de informação que o modelo CHAPAS fornece ao cidadão, contrasta com o que acontece na prestação dos serviços OEV controlada por

instituições, porque nestas (i) as trocas de informação entre instituições podem não ser apercebidas pelo cidadão, o que levanta questões de privacidade porque o cidadão tem o direito de saber quem acede aos seus dados pessoais, que informação é acedida e por que razão é acedida, e (ii) os mecanismos que permitem a um cidadão exercer o direito de verificação dos seus dados pessoais implicam normalmente processos complicados que na prática desincentivam o cidadão de o fazer.

Por outro lado, a acumulação de informação excessiva sobre os cidadãos promove nestes a existência de sentimentos de preocupação em relação ao respeito pela sua privacidade e gera desconfianças em relação à atuação do Estado em geral, o que não é bom até para a própria democracia (Nissenbaum 2004). O modelo CHAPAS em si não fornece mecanismos para que o cidadão possa expressar essas preocupações, mas permite que o cidadão tenha informação que pode usar para fundamentar as suas preocupações, ao manifestá-las nos locais adequados para o efeito.

O modelo CHAPAS disponibiliza mecanismos que permitem a minimização da informação disponibilizada pelo cidadão ao mínimo indispensável para a prestação dos serviços pretendidos. A minimização da informação enquadra-se no princípio do "*need to know*" dos militares (a um sujeito apenas deve ser dada a informação necessária para realizar as suas tarefas) e da segunda lei da identidade, divulgação mínima para uma utilização restrita (Cameron 2005). No entanto, esta minimização apenas é possível com instituições sensibilizadas para a necessidade de proteção da privacidade do cidadão, no que as instituições da AP deviam ser exemplares (Lau 2003).

Estes mecanismos permitem (i) que uma instituição especifique individualmente quais os itens de informação que devem constar em cada documento por ela pedido (atributos de entidades a que o documento se refere) e (ii) que os identificadores das entidades a que os documentos se referem sejam apresentados de forma ofuscada podendo, ainda assim, ser usados para a agregação de documentos.

O primeiro destes mecanismos de minimização de dados pode eventualmente ser suportado em soluções de prestação de serviços OEV controladas por instituições, só que o cidadão não tem evidências de que tal minimização aconteça efetivamente, uma vez que a comunicação entre as instituições não decorre sob o seu controlo. Quanto ao segundo mecanismo, ele é inovador (Gomes et al. 2011) e evita que as instituições tenham conhecimento das várias identidades parciais dos cidadãos e possam com isso agregar informação (para além dos documentos que é suposto agregarem para poderem prestar os seus serviços) e criar perfis mais completos destes.

A implementação do modelo CHAPAS pode ser uma forma de combater a desconfiança dos cidadãos em relação à prestação eletrónica de serviços do Estado. Com efeito, ao permitir que o cidadão verifique por si mesmo que informação fornece ou forneceu a cada instituição e que as instituições se preocupam em pedir apenas a informação estritamente indispensável para a prestação dos serviços pretendidos pelo cidadão, o modelo CHAPAS constitui-se como um ótimo veículo para difundir as boas práticas do Estado em relação ao processamento e tratamento de informação e, dessa forma, fomentar a confiança dos cidadãos, não só na prestação eletrónica de serviços do Estado, mas também no Estado em geral.

No entanto, apesar dos contributos para a privacidade dos cidadãos promovidos pelo modelo CHAPAS, é importante mencionar que há aspetos que lhe escapam e que podem ter grande impacto sobre a privacidade dos cidadãos. Um primeiro aspeto é que o modelo CHAPAS apenas desincentiva a existência de diálogos diretos entre instituições que envolvam a troca de informação dos cidadãos mas, de todo, não garante que eles não possam acontecer. Um segundo aspeto, de alguma forma relacionado com o primeiro, é que o modelo CHAPAS não garante que a informação fornecida pelo cidadão a uma instituição seja exclusivamente usada para a finalidade anunciada pela instituição, que tipicamente será a prestação do serviço pretendido pelo cidadão. Estes aspetos ultrapassam o âmbito da tecnologia e estão relacionados com o respeito, ou falta dele, das instituições pelos cidadãos que nelas confiaram ao fornecer a sua informação.

Uma forma como as instituições fomentam a confiança dos cidadãos nas suas práticas é através da divulgação das suas políticas de privacidade, onde manifestam qual a utilização a dar aos dados fornecidos e adquiridos, se a informação fornecida pode, ou não, ser disponibilizada a entidades terceiras, quais os mecanismos implementados para promover a segurança da informação fornecida, etc. No entanto, pode haver desfasamentos entre o anunciado e a realidade (Dias et al. 2013). À semelhança do que acontece com as políticas de privacidade, também a implementação do modelo CHAPAS poderá não significar um verdadeiro empenhamento das instituições na privacidade dos cidadãos. No entanto, mesmo que isso aconteça, o cidadão fica sempre com o registo exato da informação que disponibiliza, a quem, quando e em que contexto, e pode com isso fazer os seus juízos de valor relacionados com o conhecimento que as instituições revelam ter sobre si.

3.9.5 *INCENTIVO AO DESENVOLVIMENTO DE NOVAS APLICAÇÕES PARA APOIO AO CIDADÃO*

Um aspeto que nos parece importante realçar é que o modelo CHAPAS tem o potencial de promover o desenvolvimento de novas aplicações para auxiliar o cidadão na obtenção de serviços das várias instituições. Uma vez que os serviços estão publicamente acessíveis, são baseados em tecnologia aberta e normalizada, e as suas interfaces e políticas também são públicas, tanto os cidadãos como empresas podem desenvolver novas formas de interagir com as instituições, eventualmente explorando aspetos pouco desenvolvidos neste trabalho como a usabilidade, a exploração de dados associados aos vários serviços obtidos, adoção de ontologias que permitam a gestão da informação do cidadão, etc. Note-se que nada impede que o Chappie deixe de ser agnóstico em relação a determinados documentos, e isso pode permitir o desenvolvimento de versões orientadas para determinados serviços OEV que incluam funcionalidades específicas apenas possíveis conhecendo a semântica do conteúdo dos documentos envolvidos no serviço.

Este aspeto do incentivo ao desenvolvimento de novas aplicações e funcionalidades, regra geral, não é explorado nos modelos de prestação de serviços integrados, uma vez que o controlo fica todo do lado das instituições. No entanto, pode ser uma alavanca importante para o incentivo à adoção da prestação eletrónica de serviços. Note-se que o investimento no desenvolvimento do Chappie não fica necessariamente do lado da AP, podendo o seu desenvolvimento ser aberto à comunidade. Assim, potencia-se a concorrência entre Chappies e a inclusão de novas funcionalidades o que pode ser interessante para a renovação da prestação de serviços sem envolver grandes custos do lado da AP.

3.9.6 *INTERAÇÕES COM EMPRESAS*

O modelo CHAPAS foi concebido tendo como objetivo servir o cidadão nas suas interações com a AP, i.e., a realização de interações designadas como G2C. Não foi estudada a sua utilização para interações de empresas com a AP (G2B). No entanto, parece-nos que essa utilização poderá também ser de interesse para as empresas, devido ao controlo do fluxo de dados e aos mecanismos de minimização de dados que o modelo CHAPAS disponibiliza.

Adicionalmente, existem cenários em que pode ser a própria AP a tirar partido dos mecanismos de minimização de informação fornecidos pelo modelo CHAPAS. Por exemplo, para a realização de concursos de aquisição de bens com propostas não identificadas, i.e., em que as todas as propostas dos vários concorrentes seriam submetidas com os atributos de identidade ofuscados. Desta forma a análise das propostas seria feita sem o conhecimento das identidades dos proponentes. A revelação das identidades dos concorrentes seria feita no final da apreciação com o fornecimento, por parte dos concorrentes, dos parâmetros de ofuscação usados para ofuscar os atributos de identidade.

Um aspeto não despiciendo do cenário atrás mencionado é que a parte mais interessada na utilização das características do modelo passa a ser a própria AP e não os seus clientes, como acontece na maioria dos cenários normais de utilização. Este aspeto é algo surpreendente porque pode ser usado para fomentar o interesse da própria AP no modelo CHAPAS e alavancar a sua divulgação, o que à partida não antecipávamos.

3.9.7 FALHAS NA PRESTAÇÃO DE SERVIÇOS

Falhas sempre acontecem e podem acontecer pelas mais variadas razões. Por isso, são algo com que devemos contar. Por exemplo, podem acontecer nas instituições, durante o processamento de um serviço pedido por um cidadão, como podem acontecer no Chappie, quando o resultado da obtenção de um serviço de alguma forma não se enquadra no esperado. Em ambos os casos a outra parte deve ser informada da ocorrência da falha, o que significa que as instituições devem notificar o cidadão da eventual ocorrência de uma falha no processamento do serviço e, caso alguma instituição esteja na origem de alguma falha detetada pelo Chappie, deve ser disso notificada, eventualmente incluindo uma mensagem introduzida pelo cidadão.

O principal problema com a ocorrência de falhas no modelo CHAPAS é possibilidade de ocorrerem no contexto da obtenção de serviços OEV, i.e., no contexto da obtenção de um conjunto de serviços que apenas faz sentido quando todos são obtidos. Ou seja, uma falha na obtenção de um serviço põe em causa os resultados dos serviços já obtidos e a obtenção dos restantes. Este problema não é um problema novo em sistemas de informação e uma estratégia para lidar com ele é a utilização de transações (*transactions*), em que o resultado de um conjunto de operações, que constituem a transação, se torna permanente (*commit*) se todas as operações individualmente forem

executadas com sucesso, ou todas as operações são desfeitas (*rollback*), como se nenhuma tivesse ocorrido, se alguma das operações falhar.

Esta poderá ser uma limitação significativa do modelo CHAPAS porque nos parece que as instituições dificilmente aceitarão a utilização de transações geridas pelo cidadão, no contexto do Chappie, uma vez que implicaria a devolução de serviços já obtidos pelo cidadão, em caso de falha, serviços esses que eventualmente nem foram os responsáveis pela falha. Além do mais, a devolução de serviços implicaria alguma forma de revogação dos documentos já emitidos, uma vez que estes deveriam ser declarados como inválidos, o que implica a implementação de uma infraestrutura para a revogação de documentos, o que é de difícil implementação e eventualmente terá de envolver alguma forma de comunicação entre instituições, precisamente o que se pretende evitar.

Assim, dada a não adequação das transações ao modelo CHAPAS, a solução para a ocorrência de falhas na obtenção de um serviço OEV deve passar pela tentativa de resolução da causa para a mesma, através do diálogo com a instituição cujo serviço provocou/reportou a falha, através de canais de assistência ao cidadão, e, após resolução, pelo retomar da obtenção do serviço OEV a partir do ponto de falha.

Um aspeto importante na prestação de serviços é a completude da informação fornecida. A falta de um qualquer item de informação no pedido de um serviço gera uma falha que faz com que seja necessária a sua repetição, com a inclusão da informação em falta. Provavelmente, em muitas das interações do cidadão para a obtenção de serviços, a maioria das falhas deve-se a má comunicação/interpretação de qual a informação que o cidadão deve fornecer no pedido do serviço, o que frequentemente gera desconforto e desagrado, principalmente no cidadão. No modelo CHAPAS, a publicitação por parte das instituições dos requisitos de cada serviço, na respetiva RDP, expressos formalmente e de forma passível de ser interpretada pelo Chappie, vem contribuir para que o pedido de um serviço apenas ocorra quando todos os documentos necessários já foram coletados. Desta forma, parece-nos que o modelo CHAPAS pode contribuir para a diminuição da ocorrência de falhas por falta de documentação ou fornecimento de documentação errada.

3.9.8 AUTENTICAÇÃO

A autenticação é um aspeto de extrema importância na prestação de serviços, porque permite a uma entidade verificar a autenticidade da identidade de um seu interlocutor. Obviamente, por lidarem com informação pessoal, para muitos serviços da

AP é fundamental conhecer com rigor a identidade do cidadão com quem estão a interagir. De igual modo, para o cidadão é importante ter a certeza que está a aceder ao serviço pretendido, prestado pela entidade legítima, e não a ser vítima de um logro. Ou seja, é fundamental a autenticação mútua das partes envolvidas na prestação de serviços: do cidadão e das instituições prestadoras de serviços.

A autenticação é uma área muito vasta da segurança informática que claramente extravasa o âmbito deste trabalho. No entanto, dada a sua importância para a prestação de serviços, é necessário abordar alguns aspetos da sua utilização no contexto do modelo CHAPAS. Um primeiro aspeto é que a comunicação do Chappie com os servidores que prestam os serviços pretendidos pelo cidadão deve ser realizada através de canais de comunicação seguros que envolvam a autenticação do servidor. A tecnologia SSL/TLS, em que o servidor se autentica através de um certificado digital de chave pública, é a mais comum para o estabelecimento de canais de comunicação seguros e pode perfeitamente ser usada no modelo CHAPAS.

Para a autenticação do cidadão perante uma instituição que forneça um serviço por ele pretendido, pode ser usado qualquer protocolo de autenticação, desde que o Chappie o suporte. Só que, devido ao carácter, de algum modo, "intrusivo" da autenticação, que obriga o cidadão a ter de explicitamente comprovar algum fator de autenticação (e.g., o conhecimento de algum segredo, como um PIN ou uma senha, e/ou a posse de algum dispositivo, como um *smart card*, e/ou alguma característica biométrica, como a impressão digital), é conveniente ter em conta o eventual incómodo criado por múltiplas autenticações sucessivas quando se acede a um conjunto de serviços. Para cidadãos que pretendam um maior grau de controlo sobre o acesso aos serviços, a existência destas múltiplas autenticações explícitas não é um problema, a menos da natural dificuldade na gestão de muitas credenciais de autenticação. No entanto, para cidadãos que privilegiem a comodidade, a autenticação explícita frequente pode não ser adequada, fazendo sentido a utilização de uma funcionalidade de *Single Sign-On* (SSO). Com esta funcionalidade, o cidadão autentica-se explicitamente perante uma instituição fornecedora de identidade (*Identity Provider* - IdP), que depois, dentro de certas condições (e.g. dentro de um determinado limite temporal), emitirá credenciais ou asserções garantindo a identidade do cidadão para outras instituições que nela confiem, sem que o cidadão tenha necessidade de novamente se autenticar de forma explícita.

Existem múltiplos mecanismos e protocolos para a autenticação explícita do cidadão. Evidentemente o Chappie irá ter de suportar alguns e, qualquer que eles sejam, será com certeza necessário adaptar o Chappie para a sua utilização.

Quanto à utilização de SSO, parece-nos importante que este não seja baseado na comunicação direta entre instituições, mas sim que siga o paradigma da comunicação entre instituições do modelo CHAPAS, i.e., a comunicação deve ser feita através do Chappie. Por exemplo, o *Information Card Model*, apresentado na secção 2.4.2, segue este modelo de comunicação. Neste contexto, a utilização de asserções para veicular a identidade do cidadão, parece-nos interessante por duas razões: primeiro porque uma asserção não é mais do que um documento que contém um conjunto de atributos e, como tal, pode ser encarado como mais um documento que o cidadão tem de obter para apresentar no pedido para a obtenção de um serviço, o que possibilita uma grande flexibilidade na seleção/utilização dos atributos a usar, permitindo inclusive a utilização de atributos ofuscados. A segunda razão é a possibilidade de inclusão nas asserções de uma chave pública de um par de chaves na posse do cidadão, como mais um atributo do cidadão. Este par de chaves, eventualmente de curta duração temporal, pode ser usado para assinar digitalmente os pedidos de serviços feitos pelo cidadão. Desta forma, ao incluir a asserção de identidade num pedido de serviços assinado com a chave privada correspondente à chave pública na asserção, o cidadão prova a posse da asserção e prova que foi efetivamente ele que realizou o pedido, uma vez que é suposto a chave privada, ser da sua posse exclusiva[20].

Ainda em relação ao SSO, é necessário analisar um pouco mais os atributos a incluir nas asserções de identidade. Estes atributos tipicamente são os identificadores pelos quais o cidadão é identificado na instituição prestadora do serviço em que a asserção vai ser usada, que podem diferir dos identificadores pelo qual o cidadão é identificado noutras instituições. Assim, para poder prestar um serviço de autenticação SSO em contextos de múltiplas instituições que reconhecem diferentes identificadores do cidadão, um IdP tem de ter conhecimento desses vários identificadores do cidadão e, de alguma forma, ter verificado a legitimidade da sua pertença ao cidadão em causa. Isto implica que os IdP funcionem como "notários" nos quais os cidadãos confiam para guardar e agregar

[20] A existência de asserções contendo chaves públicas em que a entidade a autenticar deve provar a posse da correspondente chave privada, está previsto na norma SAML (Ragouzis et al. 2008) e são asserções que devem incluir o elemento "<*subject confirmation*>" definindo o método *holder-of-key*.

alguns dos seus atributos, e nos quais as entidades prestadoras de serviços também confiam para aceitar como verdadeiras as asserções sobre a identidade dos cidadãos. Adicionalmente, estes "notários" podem facilitar a ofuscação de identificadores do cidadão, se a instituição prestadora de um serviço confiar na entidade "notário" para verificar sem revelar os atributos de identidade não fundamentais para a prestação do serviço pretendido pelo cidadão. Note-se ainda que, tal como acontece com os verdadeiros notários, pode constituir-se uma rede de instituições "notários", podendo o cidadão escolher qual ou quais pretende usar e, escolhendo várias, pode eventualmente distribuir os seus atributos entre elas de forma que nenhuma fique na posse de um conjunto significativo dos seus atributos.

3.9.9 PAGAMENTO DE SERVIÇOS

Um aspeto importante da prestação de serviços ao cidadão é o pagamento dos serviços obtidos por este. Este assunto não foi objeto de estudo detalhado neste trabalho, mas justificam-se algumas reflexões.

É normal que um cidadão tenha que pagar pelos serviços que obtém. No caso concreto de um serviço OEV, que pode ser composto por vários serviços parciais, levanta-se a questão de como deve ser efetuado o pagamento da totalidade do serviço e de como distribuir os valores devidos a cada uma das várias instituições envolvidas.

Em soluções de prestação de serviços OEV cujo controlo é feito centralmente por uma instituição, é possível a existência de um pagamento único para todo o serviço OEV. O valor do pagamento, tipicamente, será recebido pela instituição que gere o serviço, que depois o dividirá com as restantes instituições, o que pressupõe a existência de acordos prévios entre as várias instituições envolvidas na prestação do serviço OEV, para a definição de políticas de preços e de pagamentos (interoperabilidade organizacional).

No modelo CHAPAS não é possível um pagamento único para todo o serviço OEV, uma vez que na realidade o cidadão não está a obter um único serviço mas sim um conjunto de serviços individuais, possivelmente prestados por várias instituições, que têm de ser pagos individualmente no momento da sua obtenção. Isto pode ser visto como um incómodo para o cidadão, uma vez que implica a realização de múltiplos pagamentos, com a eventual correspondente introdução de códigos para permitir a operação, mas pode também ser visto como mais um elemento de controlo, uma vez que o cidadão pode verificar o que está a pagar e a que instituições.

3.10 CONCLUSÃO

Neste capítulo definimos os objetivos pretendidos para o modelo CHAPAS para a prestação de serviços OEV ao cidadão, apresentámo-lo de forma detalhada e discutimos alguns aspetos relevantes do modelo e os seus impactos no cidadão e na própria AP.

Os objetivos pretendidos são: (i) colocar o cidadão no controlo da obtenção do serviço OEV e (ii) fomentar a redução do fornecimento de informação do cidadão às IPS para o mínimo indispensável para a prestação dos serviços por ele pretendidos.

O modelo CHAPAS caracteriza-se por permitir ao cidadão a obtenção de serviços OEV, compostos por múltiplos serviços parciais, eventualmente prestados por múltiplas instituições, em que é o cidadão, através do seu Chappie, uma aplicação que corre em ambiente controlado pelo cidadão (e.g. o seu computador pessoal), que compõe e coordena a obtenção desses múltiplos serviços parciais. Isto coloca o cidadão no centro do fluxo de informação entre as instituições necessário para a prestação do serviço OEV, o que lhe permite um efetivo controlo sobre a informação que disponibiliza a cada instituição (que informação, quando e porquê), o que satisfaz o primeiro objetivo.

Adicionalmente o modelo CHAPAS fornece mecanismos que permitem que as instituições possam reduzir a informação que pedem aos cidadãos para o mínimo estritamente necessário para a prestação do serviço, o que pode ser feito de duas formas: (i) permitindo que as instituições indiquem quais os atributos das entidades a que um documento se refere que efetivamente devem constar no documento, sendo os restantes atributos excluídos na emissão do documento, e (ii) permitindo às instituições a agregação de documentos usando atributos de identificação com valores ofuscados. Com estes dois mecanismos satisfaz-se o segundo objetivo proposto.

Apresentámos também o modo como o Chappie compõe os serviços OEV que o cidadão pretende obter. Esta composição baseia-se numa árvore de dependências, construída com base nas RDP que cada serviço disponibiliza para genericamente indicar quais os documentos que um cidadão que o pretenda obter deve fornecer. Assim, com base num serviço inicial, o designado serviço Raiz, o Chappie vai sucessivamente obter as RDP de todos os serviços parciais e assim construir a árvore de dependências. A obtenção do serviço será a posterior obtenção de todos os serviços na árvore de dependências, começando pelas folhas e terminado no serviço Raiz.

Por fim, discutimos alguns aspetos relevantes do modelo CHAPAS e os impactos do modelo na obtenção dos serviços pelo cidadão e na correspondente prestação por parte das IPS, apontando algumas vantagens e desvantagens face à prestação de serviços integrados.

4 PROVA DE CONCEITO

Depois de apresentado o modelo CHAPAS vamos agora fazer uma prova de conceito para avaliar a sua adequação à prestação de serviços OEV. Para isso selecionámos um evento da vida, a compra de casa pelo cidadão, que envolve a prestação de serviços por várias IPS, da AP e particulares, e, com base nele, desenvolvemos um cenário de exploração adequado ao modelo CHAPAS. Implementámos um protótipo do Chappie e dos serviços prestados pelas várias IPS, que utilizámos na exploração do cenário desenvolvido, com vista a avaliar as seguintes facetas do modelo:

- A viabilidade da composição de serviços OEV, modelados como árvores de dependências, com base nas RDP de cada serviço participante.
- A viabilidade da obtenção pelo Chappie dos vários serviços parciais que compõem um serviço OEV tendo em conta os vários padrões de interação e as várias intervenções do cidadão que possam vir a ser necessárias.
- A viabilidade da agregação de documentos com base em atributos ofuscados.

Assim, começamos por apresentar, na secção 4.1, o serviço OEV de compra de casa, na secção 4.2 apresentamos o cenário de exploração construído com base no serviço OEV, na secção 4.3 apresentamos alguns detalhes da implementação do protótipo, na secção 4.4 exploramos a utilização do protótipo no cenário anteriormente definido. Na secção 4.5 discutimos o resultado da prova de conceito e validamos o modelo. Por fim, na secção 4.6, fazemos um resumo do capítulo.

4.1 EVENTO DA VIDA: COMPRA DE CASA

A compra de casa é um exemplo típico de um evento da vida que afeta muitos cidadãos nalguma etapa das suas vidas. Para realizar a compra de uma casa, o cidadão tem de seguir um processo complexo, com várias etapas que envolvem interações com várias instituições da AP e eventualmente com instituições privadas. Apenas no final desse processo a compra da casa está concretizada.

As razões para a escolha da compra de casa foram (i) a sua complexidade, que nos permite explorar aprofundadamente o modelo CHAPAS, e (ii) ter o seu processo documentado num relatório do protótipo do Cartão de Cidadão (Projecto Cartão de Cidadão 2006).

De acordo com o referido relatório, o processo de compra de casa (PCC) é composto por oito etapas, ilustradas na Figura 16, e nele participam 6 entidades, para além do cidadão comprador: o Banco, o Vendedor, a Camara Municipal, as Finanças, a Conservatória do Registo Predial (CRP) e um Notário. O relatório indica ainda quais os documentos de entrada e de saída em cada etapa do processo, que por questões de legibilidade não incluímos na Figura 16, mas que são identificados na secção 4.2.1.

Entretanto, desde 2006, este processo não sofreu alterações significativas. A alteração mais importante foi a passagem do Registo Definitivo de opcional para obrigatório, cabendo a responsabilidade da sua comunicação à Conservatória do Registo Predial. Outras alterações foram a privatização dos notários e ter terminado a obrigatoriedade de realizar as escrituras perante um notário, podendo atualmente ser realizadas por outras entidades, como os advogados por exemplo.

O que entretanto ocorreu de significativo para o cidadão foi a implementação do serviço Balcão Único Casa Pronta, que está disponível em Conservatórias do Registo Predial e em Serviços de Registo, e permite ao cidadão tratar num só lugar de todos os atos da compra de casa que envolvem a Administração Pública.

Como as alterações ao PCC entretanto ocorridas não nos pareceram significativas, decidimos utilizar o PCC tal como representado na Figura 16 como base para o desenvolvimento do cenário de exploração.

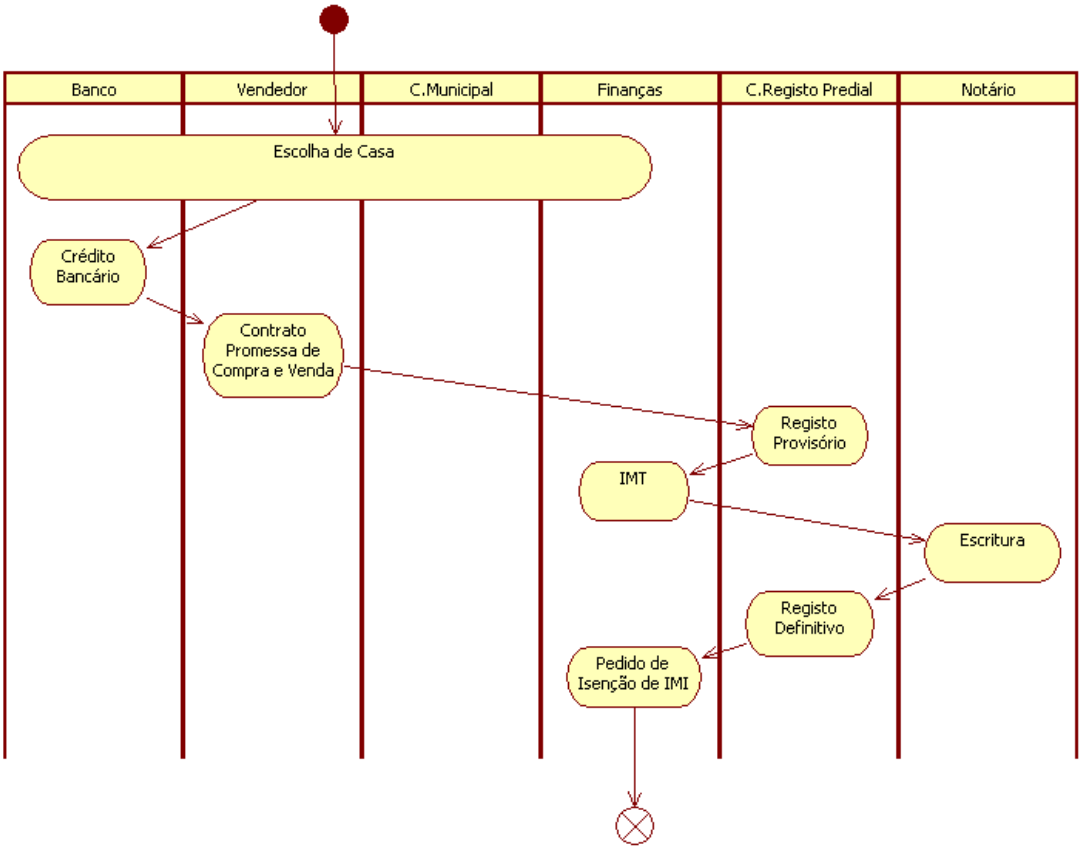

Figura 16: As principais etapas do Processo de Compra de Casa (PCC) (Projecto Cartão de Cidadão 2006)

4.2 CENÁRIO DE EXPLORAÇÃO

O cenário de exploração consiste na adequação do PCC, tal como representado na Figura 16, ao modelo CHAPAS. Nem todas as etapas do PCC ilustradas na Figura 16 foram consideradas para o protótipo, como foi o caso das etapas *Escolha de Casa* e *Crédito Bancário*. A etapa de *Escolha de Casa* não foi considerada porque não se trata propriamente de um serviço que o cidadão vá obter, mas sim de um processo mais ou menos demorado que implica negociações com vendedores e visitas a casas até que o cidadão tome a decisão final de qual a casa que pretende comprar. Quanto à etapa do *Crédito Bancário*, também não foi considerado pela mesma razão de que se trata de um processo negocial do cidadão com instituições bancárias com o objetivo de selecionar aquela que lhe oferece as melhores condições de financiamento para a compra da casa.

Quanto à etapa do *Contrato Promessa Compra e Venda*, ela não consiste propriamente num serviço que o cidadão vai obter a uma instituição, mas sim na produção

de um documento entre as duas partes (vendedor e comprador) envolvidas na transação de compra de casa, que podem ser dois cidadãos. Assim, esta etapa fica reduzida à posse pelo cidadão do documento Contrato Promessa Compra e Venda devidamente assinado pelas partes envolvidas na transação: pelo cidadão e pelo vendedor.

Quanto às duas últimas etapas do PCC, o *Registo Definitivo* e o *Pedido de Isenção de IMI*, elas consistem na obtenção de serviços adicionais ao PCC, que na altura não eram obrigatórias (o *Pedido de Isenção de IMI* continua a não ser). Ou seja, são serviços que podemos encarar como serviços complementares, que podem ou não ser obtidos pelo cidadão após a efetivação da compra da casa com a realização da escritura pública.

Quanto à etapa *Escritura*, trata-se de um serviço presencial, onde é obrigatória a presença do cidadão comprador e do cidadão ou entidade vendedora, ou seus representantes legais, pelo que o serviço não pode ser obtido de forma digital. Adicionalmente, a marcação da escritura no notário envolve um processo de agendamento que envolve as disponibilidades das várias entidades participantes (comprador, vendedor, notário e, eventualmente, o banco), podendo inclusive ser realizada fora das instalações do notário (o que normalmente acontece quando a compra de casa é feita com recurso ao crédito bancário, em que a escritura é realizada nas instalações do banco). Assim, para efeitos do cenário de exploração considerámos que a etapa *Escritura* consiste no fornecimento ao notário de toda a documentação necessária para a realização da escritura para possibilitar uma prévia análise e acelerar a escritura presencial.

Na secção seguinte, secção 4.2.1, iremos identificar as várias IPS participantes no cenário de exploração, bem como os vários serviços por elas prestados e os documentos de que cada serviço depende bem como os que cada um dos serviços emite. Abordamos também a inclusão no cenário de exploração de um conjunto de características da prestação de serviços, como a dependência de alguns serviços em relação a circunstâncias do cidadão, na secção 4.2.2, o pagamento dos serviços, na secção 4.2.3, a autenticação, na secção 4.2.4, a agregação de documentos com base em atributos ofuscados, na secção 4.2.5, os padrões de interação com os vários serviços, na secção 4.2.6, a introdução de dados diretamente pelo cidadão, na secção 4.2.7 e a existência de documentos produzidos pelo cidadão, na secção 4.2.8.

4.2.1 IDENTIFICAÇÃO DOS SERVIÇOS E DOCUMENTOS

Como a etapa *Escritura* é o último serviço do PCC, aquele cuja obtenção marca o final do processo (i.e., a concretização da compra da casa pelo cidadão), significa que se trata do último serviço crucial do PCC e, portanto, o serviço desta etapa deve ser o Serviço Raiz para a obtenção do serviço compra de casa de acordo com o modelo CHAPAS. Devido a esta etapa ficar reduzida à submissão dos documentos necessários para a realização da escritura, designamos o serviço como *Submissão de Documentos para Escritura Pública*.

Para a identificação dos vários documentos e serviços envolvidos no cenário de exploração, construímos a árvore de dependências que corresponde diretamente ao PCC da Figura 16. Esta árvore de dependências está ilustrada na Figura 17 e tem como Serviço Raiz o serviço *Submissão de Documentos para Escritura Pública*. Nela, indicamos a itálico os nomes dos vários serviços, a negrito os nomes das instituições que os fornecem e a negrito sublinhado os nomes dos documentos produzidos por cada serviço, que são os documentos que é necessário fornecer aos serviços que deles dependem (as setas entre serviços ilustram as relações de dependência (apontam para o serviço de que se depende).

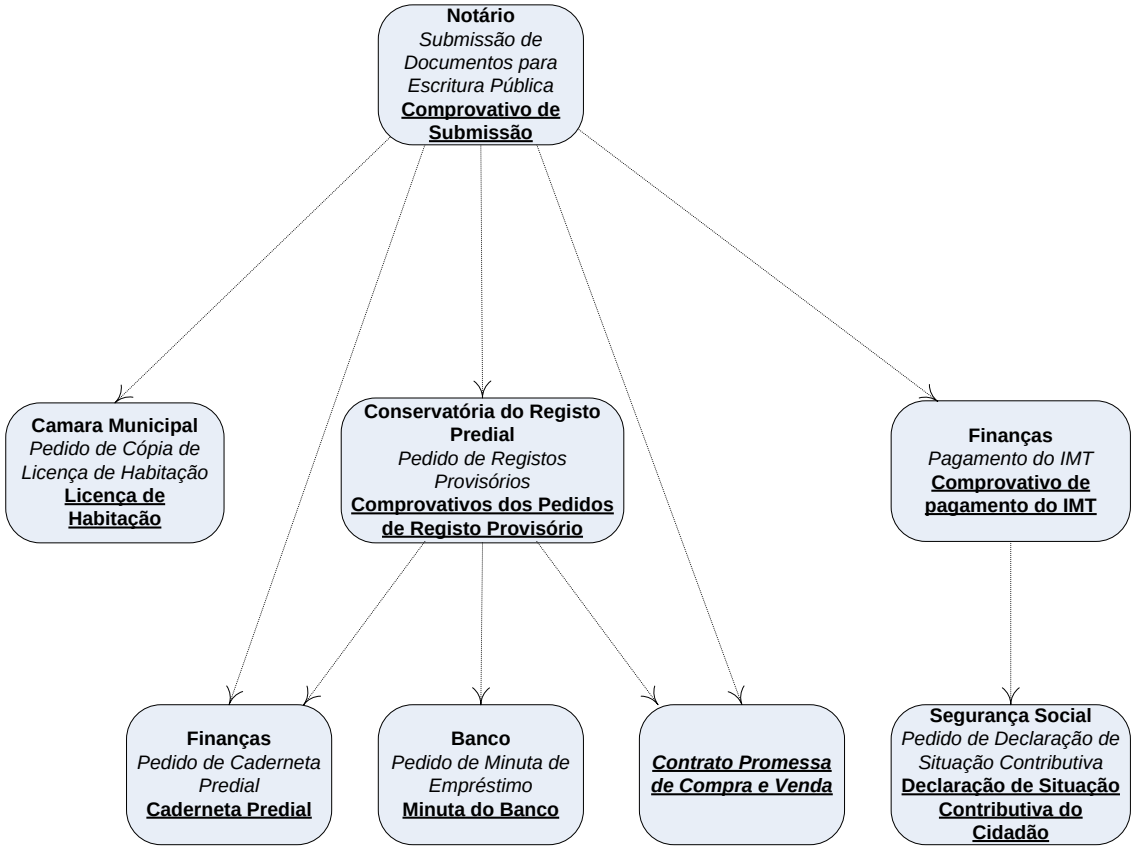

Figura 17: Árvore de dependências para o serviço OEV de *Compra de Casa*.

Há alguns aspetos sobre esta árvore de dependências que importa referir: (i) em primeiro lugar, nela não estão indicados os documentos a produzir pelo cidadão que alguns serviços pedem. Isso acontece com o serviço *Pagamento de IMT*, em que o cidadão tem de preencher e entregar o formulário **Declaração para Liquidação** (Modelo 1 e Anexos), e com o serviço *Pedido de Registo Provisório*, em que o cidadão tem de preencher e entregar o formulário **Pedido de Registo**; (ii) em segundo lugar, considerámos que o documento **Comprovativo do Pedido de Registos Provisórios**, produzido pela **Conservatória do Registo Predial**, inclui a **Certidão de Teor** da respetiva casa, pelo que não incluímos na árvore de dependências um serviço específico para obter essa certidão; (iii) em terceiro lugar, a árvore de dependências não reflete a dependência do serviço *Pedido de Registos Provisórios* da circunstância do cidadão ter ou não recorrido a um empréstimo bancário; (iv) em quarto lugar, a árvore de dependências não inclui nenhum serviço para a realização dos pagamentos que o cidadão tem de realizar para obter alguns dos serviços; (iv) por último, a árvore de dependências não inclui nenhum serviço para a autenticação do cidadão.

Após a inclusão dos resultados da análise dos três últimos aspetos atrás indicados, que são abordados nas secções seguintes, obtemos a árvore de dependências final para o cenário de exploração do evento da vida Compra de Casa que se ilustra na **Erro! A origem da referência não foi encontrada.**.

4.2.2 CIRCUNSTÂNCIAS DO CIDADÃO

Existem serviços que dependem das circunstâncias de cada cidadão em concreto. No PCC, esta dependência de circunstâncias do cidadão ocorre no serviço *Pedido de Registos Provisórios*, onde apenas os cidadãos que tenham recorrido ao crédito bancário têm de fornecer o documento **Minuta do Banco**.

Analisando mais em pormenor esta circunstância de o cidadão ter ou não pedido um empréstimo bancário, podemos argumentar que o serviço *Submissão de Documentos para Escritura Pública* também depende da mesma circunstância. De facto isso acontece e é relevante essencialmente para os aspetos de agendamento da escritura e para o fornecimento pelo banco do documento complementar que regula os termos do empréstimo. No entanto, olhando apenas pelo ponto de vista do cidadão, a dependência dessa circunstância para o fornecimento dos documentos deixa de fazer sentido se a **CRP** emitir num documento único os comprovativos de todos os registos provisórios que o

cidadão tenha feito referentes ao imóvel a adquirir (o registo provisório de aquisição que é sempre necessário e o registo provisório de hipoteca no caso de se tratar de uma compra de casa com recurso a empréstimo bancário). Assim, com base neste pressuposto consideramos que o serviço *Pedido de Registos Provisórios*, prestado pela **Conservatória de Registo Predial**, emite sempre dois documentos: a **Certidão de Teor** e o **Comprovativo dos Pedidos de Registos Provisórios**.

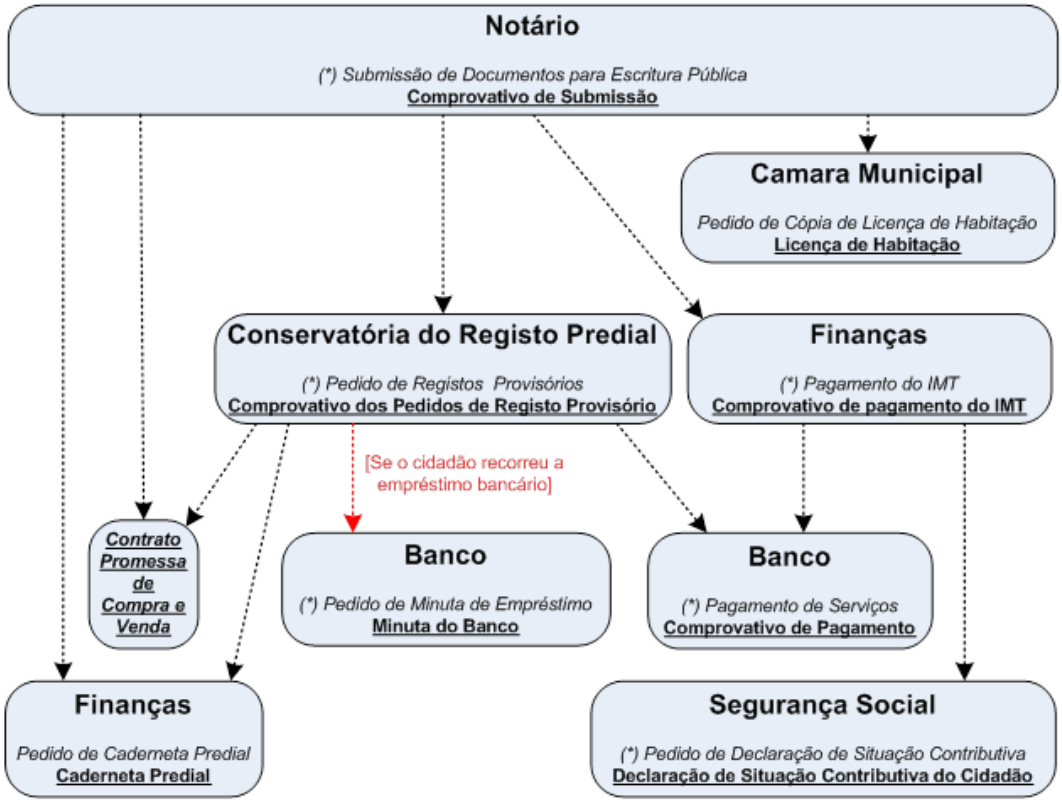

Figura 18: Árvore de dependências final para o cenário de exploração do evento de vida Compra de Casa. As setas indicam dependências entre serviços. Os nomes das IPS estão indicados a negrito, os nomes dos serviços a itálico e os nomes dos documentos produzidos são indicados a negrito sublinhado. O sinal (*) antes do nome de um serviço indica que o serviço precisa da autenticação do cidadão.

4.2.3 PAGAMENTOS

Um serviço que considerámos importante incluir no cenário de exploração é um serviço para a realização de pagamentos, a prestar por uma instituição bancária. Com efeito, da análise que fizemos aos serviços, verificámos que o pagamento é um elemento de relevo nos serviços *Pedido de Registo Provisório* e *Pagamento de IMT*, pelo que não faz

qualquer sentido incluir esses serviços no cenário de exploração sem incluir a possibilidade de realizar os respetivos pagamentos.

Quanto aos restantes serviços na árvore de dependências, considerámos que os respetivos pagamentos podem ser omitidos do cenário, pelas seguintes razões: (i) quanto aos serviços *Pedido de Cópia de Licença de Habitação*, *Pedido de Certidão de Teor*, *Pedido de Caderneta Predial* e *Pedido de Declaração de Situação Contributiva*, porque se tratam de serviços meramente informativos e porque nalguns casos até já são prestados *online* sem custos, como acontece com pelo menos com os serviços *Pedido de Declaração de Situação Contributiva* e *Pedido de Caderneta Predial*; (ii) quanto ao serviço *Pedido de Minuta de Empréstimo*, que é prestado pelo **Banco** do cidadão, porque considerámos que o custo pode ser debitado diretamente na conta bancária do cidadão e (iii) quanto ao serviço de *Pedido de Marcação de Escritura* porque considerámos que sendo a realização da escritura um ato presencial, faz sentido que o pagamento seja realizado no ato.

Apesar de porventura poder haver vários mecanismos de pagamento, que não foram estudados no âmbito deste trabalho, para o cenário de exploração considerámos o serviço *Pagamento de Serviços*, prestado por uma entidade bancária, que aceita como entrada um documento com os dados para realizar o pagamento, fornecido pelo serviço que o cidadão pretende obter, e que emite como resultado um documento, **Comprovativo de Pagamento**, que o cidadão tem de fornecer para obter o serviço pretendido.

4.2.4 AUTENTICAÇÃO

Previamente, na secção 3.9.8, discutimos a importância da autenticação do cidadão na prestação de serviços e a utilidade da existência de um serviço de SSO para diminuir o número de autenticações explícitas do cidadão no acesso aos vários serviços parciais que compõem um serviço OEV. Sugerimos também que o serviço de SSO poderia ser baseado em asserções de identidade que incluiriam uma chave pública do cidadão, cuja correspondente chave privada seria usada para assinar digitalmente os pedidos de serviços (a asserção de identidade é um dos documentos fornecidos no pedido) e dessa forma fazer prova da identidade do cidadão. Adicionalmente, como as diferentes instituições podem usar diferentes atributos do cidadão para o identificar no acesso aos seus serviços, considerámos que faria sentido a existência de entidades "notário" (da confiança dos cidadãos e das várias instituições) para verificar e armazenar atributos do

cidadão, geridos/fornecidos por outras instituições ou pelo próprio cidadão, para depois incluir em asserções sobre a identidade deste.

Em consonância, incluímos no cenário de exploração uma instituição "notário" que presta o serviço *Asserção de Identidade* com a função de emitir asserções de identidade do cidadão para serem usadas na autenticação do cidadão no pedido de serviços das outras instituições e, assim, implementar um mecanismo de SSO. Os pedidos destas asserções de identidade ao "notário" incluem uma chave pública, para ser incluída na asserção, sendo a prova da posse da correspondente chave privada realizada com uma solicitação adicional em que o "notário" pede ao cidadão para assinar um valor aleatório (*nonce*) com a correspondente chave privada. A autenticação do cidadão nos pedidos dos vários serviços é feita através da assinatura digital desses pedidos usando a chave privada correspondente à chave pública contida na asserção de identidade contida no pedido.

Mas, para que o cidadão possa obter asserções de identidade no "notário", também é necessário que se autentique perante este. Para esta autenticação considerámos usar um PIdP (Zúquete et al. 2014), um IdP pessoal que que consiste num serviço local ao cidadão (que corre na sua máquina) que é capaz de interagir com o Cartão de Cidadão para produzir assinaturas digitais para autenticar o cidadão. O PIdP, cuja sequência de interações para a autenticação está ilustrada na Figura 19, foi concebido para ser utilizado em ambiente Web, sendo os pedidos de autenticação feitos através de redireccionamentos HTTP para a máquina local. No entanto, poderá ser alterado para funcionar de acordo com o modelo CHAPAS, como um serviço na máquina do cidadão que recebe como entrada um documento contendo um atributo com um valor para assinar e que como saída emite um documento contendo: a assinatura digital do valor recebido, o certificado digital do Cartão de Cidadão que produziu a assinatura e, eventualmente, outros dados do cartão caso sejam necessários para ser incluídos em asserções (e.g., números de identificação, morada, fotografia, etc.). A vantagem da utilização do PIdP será a de libertar o Chappie dos aspetos relacionados com os mecanismos de autenticação, ficando o PIdP responsável por lidar com eles, disponibilizando uma interface de acordo com o modelo CHAPAS.

No entanto, decidimos não o usar o PIdP no cenário de exploração por não termos explorado suficientemente a autenticação no modelo CHAPAS. Assim, o cenário de exploração inclui uma entidade "notário" para fornecer asserções de identidade para identificar e autenticar o cidadão no pedido de serviços das várias instituições mas, quanto à autenticação do cidadão nos pedidos destas asserções de identidade, ela é feita através da assinatura digital do pedido usando o Cartão de Cidadão.

Analisando agora os vários serviços na árvore de dependências para o cenário de exploração, verificamos que a autenticação do cidadão é necessária pelo menos em seis serviços, que são prestados por cinco instituições diferentes (apenas o **Banco** presta dois serviços que necessitam de autenticação).

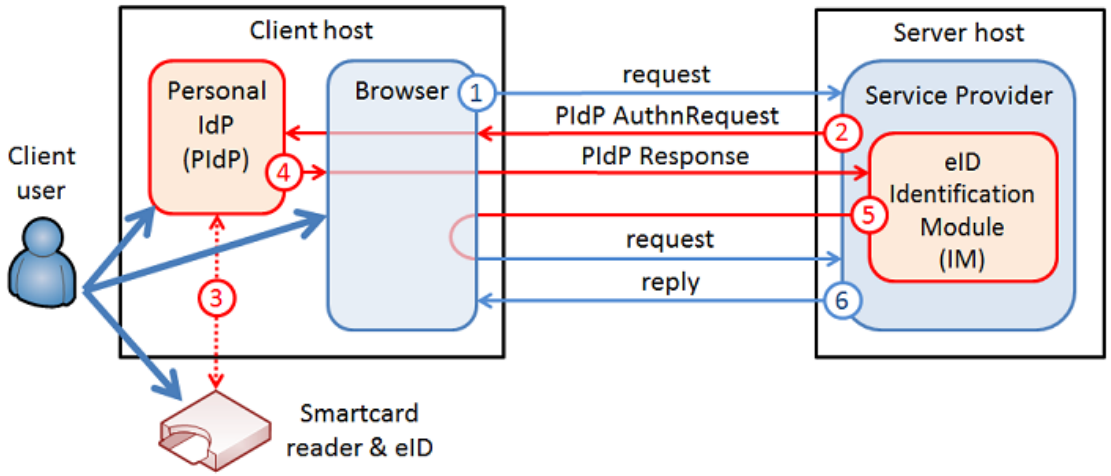

Figura 19: Arquitetura de autenticação ilustrando o posicionamento do PIdP (*Personal IdP*) e a sequência de interações envolvidas na sua utilização (Zúquete et al. 2014).

Restam pois apenas dois serviços em que podemos considerar que a autenticação do cidadão não é uma condição necessária para a obtenção do serviço. Estes serviços são: (i) o *Pedido de Cópia de Licença de Habitação*, prestado pela **Camara Municipal** e (ii) o *Pedido de Caderneta Predial*, prestado pelas **Finanças**. Estamos a considerar, apesar de ser discutível, que a informação que consta nesses documentos é pública e que não é pessoal (refere-se à casa, apesar de a **Caderneta Predial** identificar o respetivo proprietário), pelo que, por questões de transparência, não deve haver restrições no seu acesso nem haver necessidade de monitorizar quem lhe acede.

Em relação à autenticação no acesso aos dois serviços do **Banco**, consideramos que ela é feita pelo próprio **Banco** usando o tradicional esquema de nome de utilizador e senha, seguido de uma posterior inserção de três caracteres de um cartão matriz na posse do cidadão, normalmente usada nas operações da banca *online*. Esta autenticação ocorre sempre que o cidadão acede a um serviço do **Banco**, não havendo nenhum esquema de SSO.

Quanto aos restantes quatro serviços que necessitam de autenticação do cidadão, verificamos que a identificação do cidadão é realizada através de três identificadores, todos eles presentes no seu Cartão de Cidadão. São eles, o NIC (Número de Identificação

Civil), o NIF (Número de Identificação Fiscal) e o NISS (Número de Identificação da Segurança Social). Assim, considerámos que a identificação nestes serviços deve ser feita por asserções de identidade, emitidas pelo "notário", devendo estas incluir os identificadores do cidadão que cada serviço necessita. Por serviço, considerámos que a asserção de identidade para a autenticação na **CRP** para o *Pedido de Registos Provisórios* deve incluir o NIC e o NIF, que para a autenticação nas **Finanças** para o *Pagamento do IMT* deve incluir o NIF e o NISS, que para a autenticação na **Segurança Social** para o *Pedido de Declaração de Situação Contributiva* deve incluir apenas o NISS e que para a autenticação no **Notário** para a *Submissão de Documentos para Escritura Pública* deve incluir o NIC e o NIF.

4.2.5 AGREGAÇÃO DE DOCUMENTOS COM BASE EM ATRIBUTOS OFUSCADOS

A agregação de documentos com base em atributos ofuscados é uma característica do modelo CHAPAS e como tal não existe no PCC que usámos como base para a definição do cenário de exploração. Para a incorporar no cenário de exploração, foi necessário selecionar um serviço em que a sua utilização fizesse sentido.

O serviço selecionado foi o *Pagamento do IMT*, prestado pelas **Finanças**, que tem como entrada o documento *Declaração de Situação Contributiva do Cidadão*, emitido pela **Segurança Social**, que declara se o cidadão tem ou não dívidas à **Segurança Social**. Considerámos que as **Finanças** não têm uma necessidade estrita de conhecer o NISS do cidadão para permitir que este faça o pagamento do IMI. Precisa sim de saber que o cidadão que pretende pagar o seu IMT não possui dívidas à **Segurança Social**, qualquer que seja o seu NISS. De igual forma, a **Segurança Social** não precisa de saber o NIF do cidadão para emitir a respetiva *Declaração de Situação Contributiva do Cidadão*.

Assim, decidimos que a *Declaração de Situação Contributiva do Cidadão* deveria conter o NISS do cidadão de forma ofuscada. Isto implica que a asserção de identidade com que o cidadão se autentica para aceder ao serviço de *Pagamento do IMT* deverá conter o NISS ofuscado, para além do NIF em claro. Desta forma, garante-se que as **Finanças** conseguem saber se o cidadão tem ou não dívidas à **Segurança Social**, sem que com isso tome conhecimento do seu NISS.

4.2.6 PADRÕES DE INTERAÇÃO

Os padrões de interação dos vários serviços com o cidadão (Chappie) são algo que é importante considerar no cenário de exploração, devido ao impacto que têm no serviço OEV visto na sua globalidade. Por exemplo, a existência de serviços assíncronos implica serviços OEV com potencial longa duração temporal e porventura várias intervenções do cidadão, por exemplo para se autenticar.

No cenário de exploração considerámos os seguintes padrões de interação: pedido-resposta síncrono, pedido-resposta com solicitação adicional síncrona e pedido-resposta com solicitação adicional assíncrona. Considerámos o padrão de interação pedido-resposta síncrono para os serviços *Submissão de Documentos para Escritura Pública*, *Pedido de Cópia de Licença de Habitação*, *Pedido de Caderneta Predial* e *Pedido de Declaração de Situação Contributiva*, uma vez que em todos eles se referem a pedidos de documentos comprovativos de situações do conhecimento das respetivas instituições e que podem ser imediatamente emitidos. Quanto ao padrão pedido-resposta com solicitação adicional síncrona, considerámos os serviços *Pedido de Minuta de Empréstimo* e *Pagamento de Serviços*, em que o **Banco** usa a solicitação adicional para confirmar a identidade do cidadão, pedindo-lhe para indicar 3 caracteres do seu cartão matriz. Considerámos ainda o serviço *Pagamento do IMT*, em que a solicitação adicional é usada para fornecer os dados para o cidadão realizar o pagamento no **Banco** e solicitar o envio do comprovativo de pagamento. Quanto ao padrão pedido-resposta com solicitação adicional assíncrona, considerámos o serviço *Pedido de Registos Provisórios*, porque o processamento do pedido de registo provisório não é imediato, sendo a solicitação adicional usada também para enviar os dados para o cidadão realizar o pagamento do serviço e pedir o envio do correspondente comprovativo.

Para além destes serviços existe a interação com o "notário" para os pedidos de asserções de identidade, em que o cidadão tem de provar que é o dono de uma chave pública, que considerámos como um padrão pedido-resposta com solicitação adicional síncrona.

4.2.7 INTRODUÇÃO DE DADOS PELO CIDADÃO

No cenário de exploração considerámos que existem situações em que é necessário que o cidadão introduza dados para incorporar nos pedidos de serviços. Estas

situações acontecem nos serviços *Pedido de Cópia de Licença de Habitação* e *Pedido de Caderneta Predial*, onde o cidadão tem de identificar a casa sobre a qual pretende a informação. Acontecem, também, na já referida autenticação no acesso aos serviços do **Banco**, onde o cidadão tem de introduzir o seu nome de utilizador, a senha e os três caracteres do cartão matriz.

4.2.8 DOCUMENTOS PRODUZIDOS PELO CIDADÃO

No cenário de exploração considerámos que o cidadão tem de produzir e fornecer três documentos. São eles o **Contrato Promessa de Compra e Venda** (CPCV), que tem de ser assinado digitalmente pelo cidadão (comprador) e pelo vendedor da casa, o **Pedido de Registo** para o pedido de registos provisórios na CRP e a **Declaração para Liquidação** para o pagamento do IMT nas Finanças.

Como um ficheiro em XML não é adequado para a manipulação por humanos, considerámos que este formato não é o adequado para os documentos produzidos pelo cidadão. Assim, estes documentos serão produzidos por normais aplicações de edição de texto, pelo que o Chappie não poderá aceder ao seu conteúdo.

4.3 PROTÓTIPO

Nesta secção apresentamos o protótipo para a exploração do cenário descrito na secção anterior. Começamos por indicar a tecnologia utilizada, na secção 4.3.1, após o que descrevemos os vários componentes do protótipo: as instituições participantes, na secção 4.3.2, as RDP dos vários serviços, na secção 4.3.3, o Chappie, na secção 4.3.4.

4.3.1 TECNOLOGIA

No modelo Chapas existem dois componentes fundamentais, o Chappie e o Prestador de Serviços, havendo múltiplas instâncias deste último componente, tantas quantas as instituições que prestam serviços de acordo com o modelo CHAPAS.

A tecnologia selecionada para a implementação dos serviços disponibilizados pelas instituições no protótipo do modelo CHAPAS foi a tecnologia Web. Mais

concretamente, os serviços disponibilizados por cada instituição foram implementados como *Web Services*. Um *Web Service* é implementado sobre um servidor Web, tal como um portal Web, só que em vez de disponibilizar páginas *Web* para serem diretamente consumidas por seres humanos, apresenta uma interface para ser acedida por aplicações cliente que, essas sim, eventualmente, transformam os dados obtidos para serem apresentados a seres humanos.

A vantagem da utilização de *Web Services* em relação a outras tecnologias, como Corba ou RMI, é serem implementados sobre tecnologia Web, o que facilita o cruzar de fronteiras das instituições (leia-se *firewalls* e outras tecnologias de proteção do perímetro das instituições). Além disso, como todos os dados são comunicados em XML, que não é mais do que texto estruturado, permite um maior nível de interoperabilidade entre tecnologias e sistemas, algo que não acontece com outras tecnologias, como as mencionadas Corba e RMI.

Os *Web Services* foram usados para implementar os serviços disponibilizados pelas várias instituições. Para a implementação do Chappie foi usada a mesma tecnologia, só que o Chappie não implementa nenhum *Web Service*, sendo sim um cliente dinâmico de *Web Services*, i.e., uma aplicação cliente que não conhece à partida quais os *Web Services* com que vai interagir.

4.3.1.1 Web Services

O desenho dos *Web Services* foi baseado no modelo SOAP por ser uma aproximação funcional, em que os serviços representam funcionalidades, em oposição à aproximação mais virada aos dados do modelo REST, em que os serviços representam operações sobre dados. Esta escolha foi natural uma vez que os serviços prestados pelas várias instituições apresentam-se mais como funcionalidades que obtemos, basta atentar nos respetivos nomes, do que como dados sobre os quais operamos. Além disso, no modelo SOAP, os *Web Services* são descritos por um ficheiro WSDL, o que encaixa no nosso conceito de RDP, o que reforçou a opção por este modelo. No entanto, não fizemos nenhuma tentativa de integração dos ficheiros WSDL e RDP.

A implementação dos *Web Services* foi feita em ambiente NetBeans[21] e com recurso à linguagem Java. Mais concretamente, começou-se com a versão 7 do *kit* de desenvolvimento da plataforma Java SE (*Java Development Kit*) da Oracle[22], o JDK7. Mais tarde migrou-se para o JDK8. Utilizaram-se também as bibliotecas externas WSDL4J[23], para lidar com documentos WSDL (*Web Services Description Language*), e Apache Santuario[24], para lidar com assinaturas digitais e cifra em XML.

A tecnologia de *Web Services* usada foi o JAX-WS[25], que vem incorporada no JDK e que dispensa a necessidade de utilizar um servidor de aplicações adicional, como o Apache Axis[26] ou o Glassfish[27], para disponibilizar os *Web Services*. A comunicação entre o Chappie e os Prestadores de Serviços é feita com base em mensagens SOAP sobre o protocolo HTTP (para o transporte das mensagens SOAP), pelo que foram também utilizadas as bibliotecas SAAJ[28] e JAXB[29], incluídas no JDK, para lidar com mensagens SOAP e com o *marshalling* de XML para Java e vice-versa, respetivamente.

4.3.2 INSTITUIÇÕES PRESTADORAS DE SERVIÇOS (IPS)

Tendo em conta o cenário de exploração, implementámos protótipos para as seis IPS que nele participam, mais um para o "notário" que faz a autenticação do cidadão. Estes protótipos foram baseados num molde comum, que foi adaptado a cada uma das sete situações, com as seguintes funcionalidades: a disponibilização da RDP de cada serviço e a disponibilização simplificada dos serviços de cada IPS.

Em termos da disponibilização da RDP, como estas são estáticas (apenas mudam quando muda alguma característica do serviço correspondente) o protótipo responde aos pedidos com o envio da RDP que previamente lê de um ficheiro e que assina digitalmente.

[21] http://www.netbeans.org
[22] http://www.oracle.com/technetwork/java/javase/overview/index.html
[23] http://sourceforge.net/projects/wsdl4j/files/WSDL4J/
[24] https://santuario.apache.org/
[25] https://jax-ws.java.net/
[26] https://axis.apache.org/
[27] https://glassfish.java.net/
[28] https://saaj.java.net/
[29] https://jaxb.java.net/

Em termos da disponibilização dos serviços, o protótipo usa documentos de resposta base que eventualmente altera para dar resposta aos pedidos (e.g., coloca valores de atributos, ofusca atributos), assina digitalmente estes documentos e assina e envia a resposta. Além disso, é feita uma validação dos documentos de entrada para verificar as condições de agregação especificadas na respetiva RDP, gerando uma falha caso não se verifiquem.

Para as assinaturas digitais usou-se assinatura digital em XML, *XML Signature* (Bartel et al. 2008), do tipo *enveloped*, i.e., em que a assinatura fica contida no documento XML assinado como um elemento imediatamente debaixo do elemento raiz do documento. As assinaturas de XML foram realizadas usando o algoritmo de assinatura com cifra RSA, *hash* SHA1 e algoritmo de canonização C14N11.

A ofuscação de atributos realizou-se com cifra contínua (simétrica), usando o algoritmo AES em modo de cifra CFB-8 (*Cipher FeedBack mode*). A escolha de cifra contínua permite que os valores ofuscados sejam da mesma dimensão que os valores originais.

4.3.3 REQUIRED DOCUMENTS POLICY (RDP)

No contexto do protótipo decidimos usar uma sintaxe própria para implementar as RDP. No entanto, existe um conjunto de normas abertas definidas pela *World Wide Web Consortium* (W3C) e pela OASIS que se destinam a definir as políticas que um *Web Service* estabelece para o seu acesso. Exemplos destas normas são a norma WS-Policy, a norma WS-SecurityPolicy, a norma WS-Addressing entre outras. Sendo a RDP também uma política, faz sentido que seja implementada de acordo com as normas atrás indicadas. A principal razão para o não fazer foi a grande quantidade de normas relacionadas com *Web Services* que seria necessário analisar detalhadamente para implementar o protótipo do CHAPAS em conformidade, o que claramente extravasa o objetivo deste trabalho. Além disso, existem vários aspetos do modelo CHAPAS que não são contemplados nessas normas, como é o caso, por exemplo, das definições de documentos, circunstâncias e regras de decisão, pelo que seria sempre necessário definir alguma sintaxe própria.

A organização global de uma RDP está ilustrada na Figura 20, onde podemos observar os seus principais blocos. Na parte remanescente desta secção apresentamos estes blocos, bem como alguns aspetos da sintaxe, baseada em XML, que criámos para a definição das RDP. Assim, começamos por apresentar, na secção 4.3.3.1, o bloco de

Informação Geral, no qual se fornece informação sobre a IPS e o serviço; na secção 4.3.3.2 apresentamos o bloco de Dados de Entrada onde se definem os dados que devem ser introduzidos diretamente pelo cidadão; na secção 4.3.3.3 apresentamos o bloco Documentos, onde se definem os documentos que o cidadão tem de fornecer para obter o serviço e que obtém como resultado do serviço, o que inclui a definição dos atributos relevantes em cada um deles e a eventual identificação dos serviços onde podem ser obtidos; na secção 4.3.3.4 apresentamos os blocos Circunstâncias e Regras de Decisão, onde se definem as eventuais circunstâncias do cidadão relevantes para a prestação do serviço e as regras de decisão cuja avaliação determina quais os documentos a apresentar/receber pelo cidadão; e, finalmente, na secção 4.3.3.5 apresentamos o bloco Assinatura Digital, que contém a assinatura digital da RDP.

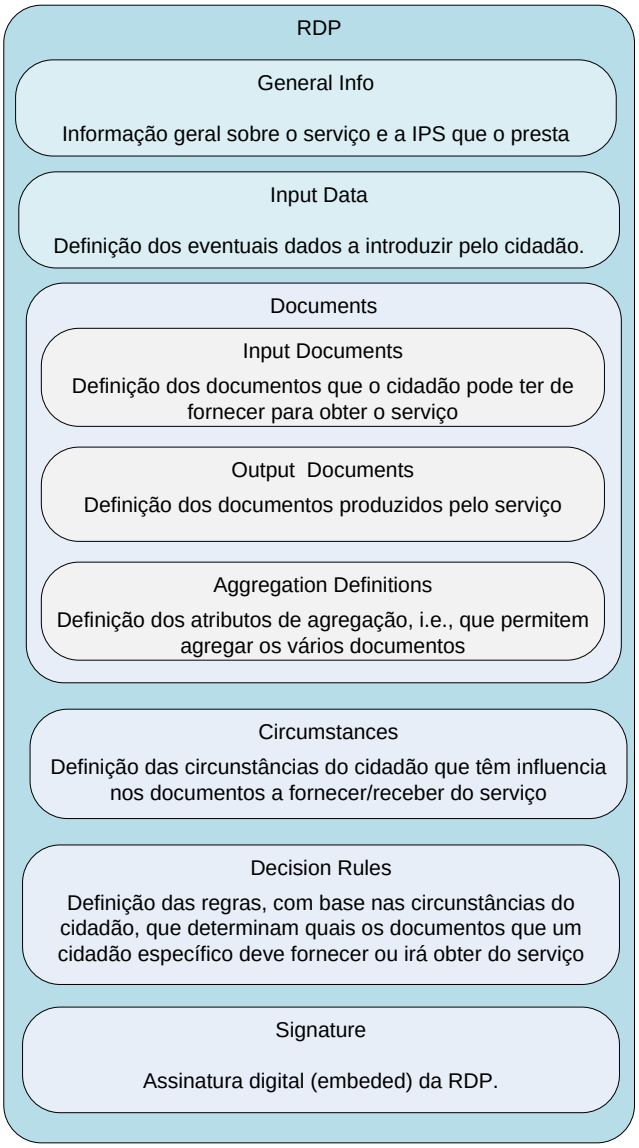

Figura 20: Organização de uma RDP (*Required Documents Policy*)

4.3.3.1 Informação Geral

Esta secção da RDP destina-se a fornecer informação de índole geral sobre o serviço e a IPS que o presta, tais como a identificação do serviço e da IPS, a indicação do endereço onde o serviço está disponível, o tipo de padrão de interação, a indicação se o pedido deve ser assinado pelo cidadão, o eventual fornecimento de uma chave a usar para cifrar eventuais conteúdos que não possam ser enviados em claro, etc. O Excerto 1 apresenta um exemplo desta secção na RDP do serviço *Pagamento de Serviços*, onde é visível a identificação do padrão de interação para a obtenção do serviço, elemento **<Interaction Pattern>** que indica tratar-se de uma interação do tipo pedido resposta síncrona com solicitação adicional, e a definição de uma chave pública, no caso concreto um certificado de chave pública, para cifrar chaves simétricas de proteção de dados que não podem ser usados em claro (dados para a identificação e autenticação do cidadão), elemento **<KeyEncriptionKey>**.

Excerto 1 Secção de informação geral sobre um serviço da RDP do serviço *Pagamento de Serviços*.

```
<ns0:GeneralInfo>
   <ns0:ServiceProvider>
      <ns0:SProviderName>Banco Único</ns0:SProviderName>
      <ns0:Description>Banco recebedor da massa no protótipo</ns0:Description>
   </ns0:ServiceProvider>
   <ns0:Service SectorName="Banca" ServiceType="Pagamentos de Serviços">
      <ns0:ServiceName>Pagamento de Serviços</ns0:ServiceName>
      <ns0:Description>Serviço de pagamentos</ns0:Description>
   </ns0:Service>
   <ns0:ServiceRequest>
      <ns0:Connection>
         <ns0:Address>http://localhost:8081/Banco/Pagamento</ns0:Address>
      </ns0:Connection>
      <ns0:InteractionPattern
                PatternType="http://www.ua.pt/Chapas/ipattern/rr-sa-sync" />
      <ns0:Encryption>
         <ns0:KeyEncryptionKey Name="EncryptionCertificate">
            <ns0:Certificate Type="X509v3" Encoding="Base64">
MIIDazCCAlOgAwIBAgIEYch+CzANBgkqhkiG9w0BAQsFADBmMQswCQYDVQQGEwJwdDEQMA4GA1UE
CBMHVW5rbm93bjEPMA0GA1UEBxMGYXZlaXJvMRAwDgYDVQQKEwdub3RhcmlvMRAwDgYDVQQLEwdV
bmtub3duMRAwDgYDVQQDEwdub3RhcmlvMB4XDTE1MDQwODE4NTU1MloXDTE1MDcwNzE4NTU1Mlow
ZjELMAkGA1UEBhMCcHQxEDAOBgNVBAgTB1Vua25vd24xDzANBgNVBAcTBmF2ZWlybzEQMA4GA1UE
ChMHbm90YXJpbzEQMA4GA1UECxMHVW5rbm93bjEQMA4GA1UEAxMHbm90YXJpbzCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBALW7a2v1HbKvvrr2NxF2gdY0v30O7sLIkauVP+ji/s2cewYR
LTZW4+szEP9U0tB+JjF6AaZ3+3a7OFYXP1R6+AXhMfm0dF2raDPHLZNTjEyZkfnH4Y7s+OK+u1/u
9/LK+UwjJ1GMTJ3TzG3n32GxFweebZAZp86ZA/d+3P0zqrpw5Cu4+uS0ansuVztEZb+zZwe9r9SN
ghOHka3AJfo/Hk4RpebNGYyFqEQs4FKNMC31fR00w3MUZWxslwaxSP0zHJG8FPmSHXa2UjfIos/o
7makHnYhgAl26an+pzw4q+bchFI92QAH1JfRPCCMirplSyA+SWkEXOVPC+I1Cndht68CAwEAAaMh
```

```
MB8wHQYDVR0OBBYEFK60CMI0u7bj2KrswsOSiAO56s+SMA0GCSqGSIb3DQEBCwUAA4IBAQArtY7q
LsRLLOBmkLotviHlJyUTdlGVf7nGfs4Onvx+QLinZCjIf8V1TYTEnIALmP4IM2w/svRRSBPkQEKJ
5SPAQOQe3UYa2bQ2J8ynkSspEFW86J9joH4Mu04WU5BCFjkC9Dz63qDEdMOqOvztqV2+D6eXgDHi
pS2anxwlnZNbBn+Pa1KtpaYfmUiENV8qycIYLCNxIIYA71RwzIzdKNJtbVtkcNazIUs/fhHILIQO
Hl6Ql4d0K9AIdscb5I37/LlEd/ftt6HwlP8YsEm/tx1tI6kjZZy2EG3FmIoycnTRv/euTUUK2lZs
+mCUNI801XJUVyBR1jioqDUGK6RmyzdE</ns0:Certificate>
         </ns0:KeyEncryptionKey>
      </ns0:Encryption>
   </ns0:ServiceRequest>
   <ns0:ServiceResponse/>
</ns0:GeneralInfo>
```

No Excerto 2 apresenta-se um outro exemplo, agora do serviço *Pagamento do IMT*, em que é visível a indicação de que os pedidos do serviço devem ser assinados digitalmente (elemento **<RequestSignature>**), bem como a identificação da chave pública para a validação das assinaturas dos pedidos e do documento que a contém (elemento **<AssercaoIdentidade>**).

Excerto 2 Secção de informação geral da RDP do serviço *Pagamento do IMT*.

```
<ns0:GeneralInfo>
  <ns0:ServiceProvider>
    <ns0:SProviderName>Finanças</ns0:SProviderName>
      <ns0:Description>Autoridade Tributária e Aduaneira</ns0:Description>
  </ns0:ServiceProvider>
  <ns0:Service SectorName="Administração Pública" ServiceType="PagamentoImpostos">
    <ns0:ServiceName>Pagamento do IMT</ns0:ServiceName>
    <ns0:Description>Serviço que permite o pagamento do imposto municipal sobre as
transações onerosas de imóveis (IMT).</ns0:Description>
  </ns0:Service>
  <ns0:ServiceRequest>
    <ns0:Connection>
      <ns0:Address>http://localhost:8085/Financas/PagamentoIMT</ns0:Address>
    </ns0:Connection>
    <ns0:InteractionPattern PatternType="http://www.ua.pt/Chapas/ipattern/rr-sa-sync"/>
    <ns0:RequestSignature>
      <ns0:PublicKey>
        <ns0:AssercaoIdentidade DocRef="F-IMT-AId-In-03" AttRef="PublicKey"/>
      </ns0:PublicKey>
    </ns0:RequestSignature>
    <ns0:Encryption>
      <ns0:KeyEncryptionKey Name="EncryptionCertificate">
        <ns0:Certificate Type="X509v3" Encoding="Base64">
MIIDuzCCAqOgAwIBAgIEaX4TXTANBgkqhkiG9w0BAQsFADCBjTELMAkGA1UEBhMCUFQxCzAJBgNVBAgTAlBUMRAw
DgYDVQQHEwdVbmtub3duMSAwHgYDVQQKExdNaW5pc3RlcmlvIGRhcyBGaW5hbmNhczEqMCgGA1UECxMhQXV0b3Jp
ZGFkZSBUcmlidXRhcmlhIGUgQWR1YW51aXJhMREwDwYDVQQDEwhGaW5hbmNhczAeFw0xNTA2MTEwMjM2MzhaFw0x
NTA5MDkwMjM2MzhaMIGNMQswCQYDVQQGEwJQVDELMAkGA1UECBMCUFQxEDAOBgNVBAcTB1Vua25vd24xIDAeBgNV
BAoTF01pbmlzdGVyaW8gZGFzIEZpbmFuY2FzMSowKAYDVQQLEyFBdXRvcmlkYWRlIFRyaWJ1dGFyaWEgZSBBZHVh
bmVpcmExETAPBgNVBAMTCEZpbmFuY2FzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmfpGVDylNoWV
```

```
nCtbTO0Dazgj6QRubLIi8/KrJvcikUoMTL70ewI7rxtFY//5s42WhKr6zlOZk2t3gNBfaTL0ovXdMWHlPorDSWz7
D88oFxMoUmmY0A2nRuJppAmJh+OJMLtTfH0QOpapUJIeWOhV1/2EWWRVraFnb9UE4vMzM/4wk1oc5NYXfOVfjr58
lo8JZH/UFGBG1unW4b0BGkDZ1Iv29ll14Q5b3Z24elB9u3Goyse+nMmQOEYnWeVLtUrcSI7SSctcX23zoLA5AGej
5e+nCjso28kWKS/BE5iQAVfL7gi6I9235dK4UY1pjtUlj+vSRwSu8kWhwEuVyFfc2QIDAQABoyEwHzAdBgNVHQ4E
FgQU+lH5CwUcb6dZkAdJuVmf6jKBuYkwDQYJKoZIhvcNAQELBQADggEBAGOHZUMVh0hsU1HtNz7LJzIGUhmNEKSe
9s0PBqqgdG7e36/oHrgBGa1BQbx6kN7oCC6BumgGnIIzmwvnCiOSfFDKSJS8bPD0pIePuKxGOGSv9hvRX4kRKNdR
xp42NkrLewdV08/cxWGhN0EWIS8t/z4v76ZQby11ZVTgQSjKvuQ053yzibJGX4wVw43wuv1NI/Z35HtbAfhM4fRV
x4gwrpHNOgAlG351Gz/ORDMxEDo/1tTAJ1G6qSbsl+fRZ8E1Nc8+rbFLSsKKU4UeKaR9zcR/JUpxSceWYXcmKLwY
h+DmP2Y+yRS1rUBcgNN1wBHJgNjQqHTX6uApiOM+h7PzPVg=</ns0:Certificate>
      </ns0:KeyEncryptionKey>
    </ns0:Encryption>
  </ns0:ServiceRequest>
</ns0:GeneralInfo>
```

4.3.3.2 Dados de entrada

Nesta secção de Dados de Entrada, definem-se os itens de dados que devem ser introduzidos diretamente pelo cidadão, i.e., dados que não são fornecidos através de documentos. Esta funcionalidade é necessária porque alguns serviços necessitam de mais dados além daqueles que são fornecidos através de documentos. Como exemplos da necessidade desta funcionalidade, temos a identificação do imóvel no *Pedido de Cópia de Licença de Habitação* e a indicação do nome de utilizador, senha e dígitos do cartão matriz no serviço *Pagamentos de Serviços*.

Para manter o Chappie agnóstico em relação aos dados pedidos pelos serviços, a especificação dos dados de entrada deve conter dois tipos de informação: (i) informação para ser fornecida ao cidadão sobre os dados que estão a ser pedidos e a respetiva finalidade e (ii) a definição do modo como os dados devem ser introduzidos, o que inclui a definição de uma máscara para a filtragem dos caracteres permitidos para cada item de dados.

Eventualmente, pode ser necessário proteger os dados de entrada, para não serem observados enquanto em trânsito, na totalidade ou parcialmente. Neste caso, a especificação dos dados de entrada deve dar esta indicação e indicar qual forma de o fazer. Um exemplo desta necessidade pode ser o envio de credenciais de autenticação como o nome do utilizador e a respetiva senha. No Excerto 3, que se refere à RDP do serviço *Pagamento de Serviços*, o elemento **<Encrypt>** indica que os dados têm de ser cifrados e que a chave de cifra deve ser enviada protegida com uma chave pública identificada pela referência "EncryptionCertificate" que deve estar definida na secção de Informação Geral da RDP, através de um elemento **<KeyEncriptionKey>.**

Excerto 3 Secção de especificação de itens de dados a introduzir pelo cidadão, na RDP do serviço *Pagamento de Serviços*.

```
<ns0:InputData>
   <ns0:Encrypt KeyEncKeyRef="EncryptionCertificate"/>
   <ns0:Description>Identificação da conta bancária que vai realizar o
pagamento.</ns0:Description>
   <ns0:IDPedido>
      <ns0:DataItem DItenID="ClientNumber" Mask="0000000">
         <ns0:Label>Número de cliente</ns0:Label>
      </ns0:DataItem>
      <ns0:DataItem DItenID="AccessCode" Mask="000000">
         <ns0:Label>Código de acesso</ns0:Label>
      </ns0:DataItem>
   </ns0:IDPedido>
   <ns0:IDSolicitacaoAdicional>
      <ns0:DataItem DItenID="MatrixDigit1" Mask="0">
         <ns0:Label>Primeiro digito do cartão matriz</ns0:Label>
      </ns0:DataItem>
      <ns0:DataItem DItenID="MatrixDigit2" Mask="0">
         <ns0:Label>Segundo dígito do cartão matriz</ns0:Label>
      </ns0:DataItem>
      <ns0:DataItem DItenID="MatrixDigit3" Mask="0">
         <ns0:Label>Terceiro digito do cartão matriz</ns0:Label>
      </ns0:DataItem>
   </ns0:IDSolicitacaoAdicional>
</ns0:InputData>
```

4.3.3.3 Definição dos Documentos

A definição de documentos foi dividida em três subsecções: uma para os documentos de entrada (a fornecer pelo cidadão), outra para os documentos de saída (produzidos pelo serviço) e uma terceira com a definição dos atributos de agregação que permitem verificar que os documentos se referem a uma mesma entidade. O Excerto 4 apresenta um exemplo da definição de documentos numa RDP, no caso concreto para o serviço *Pagamento do IMT*, em que existe agregação de documentos com base em atributos ofuscados.

Para a identificação dos documentos, elemento utilizámos três identificadores: um URI que o identifica globalmente o tipo de documento, um Id que serve para identificar o documento no contexto da RDP e um nome amigável para permitir a identificação do documento pelo cidadão, que podem ser observados nos elementos **`<InputDocument>`** e **`<OutputDocument>`**, no Excerto 4, que definem os documentos de entrada e de saída, respetivamente.

Quanto à identificação das IPS emissoras dos documentos considerámos três situações: (i) o documento ser emitido por uma única IPS bem conhecida, o que acontece, por exemplo, com a emissão da **Declaração de Situação Contributiva do Cidadão**, ilustrado no Excerto 4; (ii) que o documento pode ser emitido por um serviço de determinado tipo numa IPS de um determinado sector, o que acontece por exemplo com os pagamentos que podem ser efetuados em serviços do tipo "Pagamento de Serviços" prestados por bancos (no protótipo só existe um banco, mas o Chappie reage como se houvesse vários); (iii) que o documento pode ser emitido por qualquer IPS, como é o caso do documento com os dados para realizar um pagamento, que qualquer entidade de qualquer sector pode emitir; e por fim (iv) que o documento tem de ser produzido pelo cidadão, como é o caso do **Contrato de Compra e Venda**, por exemplo.

Para a identificação dos atributos obrigatórios e dos atributos de agregação, usamos um identificador que identifica cada atributo de forma única no contexto da RDP, um nome amigável para que o cidadão saiba o que é o atributo, o que pode ser observado nos elementos **<MandatoryDocAttribute>** no Excerto 4. Em simultâneo fornece-se uma expressão XPath que permite localizar o elemento no documento correspondente ao atributo em causa.

A definição dos atributos de agregação é feita com a indicação em cada atributo se ele é ou não um atributo de agregação e, caso seja, incluindo a identificação da respetiva unidade de agregação. Nas definições das Unidades de Agregação, elementos **<AggregationUnit>** no Excerto 4, indica-se se os respetivos atributos devem ou não ser alvo de ofuscação e, caso sejam, podem ser indicados o algoritmo e a codificação a usar.

Excerto 4 Secção de especificação de documentos na RDP do serviço *Pagamento do IMT*.

```
<ns0:Documents>
   <ns0:InputDocuments>
      <!--Declaração de situação contributiva das Segurança Social-->
      <ns0:InputDocument DocId="SS-SContrib-In-01"
                         FriendlyName="Declaração de Situação Contributiva"
                         DocURI="http://ssocial.pt/Docs/DeclaracaoSContrib">
         <ns0:Description>Documento que comprova que o cidadão não possui dívidas à
Segurança Social.</ns0:Description>
         <ns0:Providers>
            <ns0:Provider Type="IndividualProvider" >
               <ns0:IndividualProvider ProviderName="SegurancaSocial"
                        ServiceName="Serviço de Pedidos de Declaração de Situação
Contributiva">
                  <ns0:Connection>
                     <ns0:Address>
http://localhost:8085/SSocial/PedidoDSituacaoContrib</ns0:Address>
```

```
                </ns0:Connection>
             </ns0:IndividualProvider>
          </ns0:Provider>
       </ns0:Providers>
       <ns0:MandatoryDocAttributes>
          <ns0:MandatoryDocAttribute MdaId="SC-NSS"
                                     FriendlyName="Número da Segurança Social"
                                     AggregationAttr="true" AggUnitRef="NSS" >
             <ns0:XPathExpr>//*[@AttId='nss']</ns0:XPathExpr>
          </ns0:MandatoryDocAttribute>
          <ns0:MandatoryDocAttribute MdaId="SitContributiva"
                                     FriendlyName="Situação Contributiva"
                                     AggregationAttr="false" >
             <ns0:XPathExpr>//*[@AttId='sitcontributiva']</ns0:XPathExpr>
          </ns0:MandatoryDocAttribute>
          <ns0:MandatoryDocAttribute MdaId="DataSitContributiva"
                                     FriendlyName="Data da Situação Contributiva"
                                     AggregationAttr="false" >
             <ns0:XPathExpr>//*[@AttId='datasitcontrib']</ns0:XPathExpr>
          </ns0:MandatoryDocAttribute>
       </ns0:MandatoryDocAttributes>
    </ns0:InputDocument>
    <!--Declaração de modelo1 a preencher pelo cidadão-->
    <ns0:InputDocument DocId="DCA-Mod1-In-02"
                       FriendlyName="Declaração Modelo 1"
                       DocURI="http://financas.pt/docs/IMT-Mod1">
       <ns0:Providers>
          <ns0:Provider Type="CitizenProvider">
             <ns0:CitizenProvider>
                <ns0:Download>
http://localhost:8082/Financas/Download/Modelo1.doc</ns0:Download>
             </ns0:CitizenProvider>
          </ns0:Provider>
       </ns0:Providers>
       <ns0:MandatoryDocAttributes/>
    </ns0:InputDocument>
    <!--Autenticação do cidadão-->
    <ns0:InputDocument DocId="F-IMT-AId-In-03"
                       FriendlyName="Asserção de Identidade do Cidadao"
                       DocURI="http://notario.pt/Docs/AsserçãoIdentidade">
       <ns0:Providers>
          <ns0:Provider Type="SectorProvider">
             <ns0:SectorProvider SectorName="AuthenticationServices"
                                 ServiceType="EmissaoAssercaoIdentidade"/>
          </ns0:Provider>
       </ns0:Providers>
       <ns0:MandatoryDocAttributes>
          <ns0:MandatoryDocAttribute MdaId="NIF"
                                     FriendlyName="Número de Identificação Fiscal"
                                     AggregationAttr="false" >
             <ns0:XPathExpr>//*[@AttId='NIF']</ns0:XPathExpr>
```

```
            </ns0:MandatoryDocAttribute>
            <ns0:MandatoryDocAttribute MdaId="NSS"
                            FriendlyName="Número de Identificação da Segurança Social"
                            AggregationAttr="true" AggUnitRef="NSS" >
               <ns0:XPathExpr>//*[@AttId='NSS']</ns0:XPathExpr>
            </ns0:MandatoryDocAttribute>
            <ns0:MandatoryDocAttribute MdaId="PKeyCidadao"
                            FriendlyName="Chave Pública para autenticação do cidadao"
                            AggregationAttr="false" >
               <ns0:XPathExpr>//*[@AttId='PKeyCidadao']</ns0:XPathExpr>
            </ns0:MandatoryDocAttribute>
         </ns0:MandatoryDocAttributes>
      </ns0:InputDocument>
      <!--Comprovativo da realização do pagamento emitido pelo banco.Este documento deve
ser entrgue na resposta à solicitação adicional-->
      <ns0:InputDocument DocId="B-CPagamento-In-04"
                         FriendlyName="Comprovativo de pagamento"
                         DocURI="http://Banco.pt/ComprovPagamento">
         <ns0:SolicitacaoAdicional RefDocToUse="DadosPagamento"/>
         <ns0:Providers>
            <ns0:Provider Type="SectorProvider">
               <ns0:SectorProvider SectorName="Banca"
                                   ServiceType="Pagamento de Serviços"/>
            </ns0:Provider>
         </ns0:Providers>
         <ns0:MandatoryDocAttributes>
            <ns0:MandatoryDocAttribute MdaId="CP-Entidade"
                                       FriendlyName="Entidade para pagamento"
                                       AggregationAttr="true"
                                       AggUnitRef="EntPagamento" >
               <ns0:XPathExpr>//*[@AttId='Entidade']</ns0:XPathExpr>
            </ns0:MandatoryDocAttribute>
            <ns0:MandatoryDocAttribute MdaId="CP-Referencia"
                                       FriendlyName="Referencia para pagamento"
                                       AggregationAttr="true"
                                       AggUnitRef="RefPagamento" >
               <ns0:XPathExpr>//*[@AttId='Referencia']</ns0:XPathExpr>
            </ns0:MandatoryDocAttribute>
            <ns0:MandatoryDocAttribute MdaId="CP-Valor"
                                       FriendlyName="Valor para pagamento"
                                       AggregationAttr="false" >
               <ns0:XPathExpr>//*[@AttId='Valor']</ns0:XPathExpr>
            </ns0:MandatoryDocAttribute>
            <ns0:MandatoryDocAttribute MdaId="DHPagamento"
                         FriendlyName="Instante em que o pagamento foi realizado"
                         AggregationAttr="false" >
               <ns0:XPathExpr>//*[@AttId='DHPagamento']</ns0:XPathExpr>
            </ns0:MandatoryDocAttribute>
         </ns0:MandatoryDocAttributes>
      </ns0:InputDocument>
```

```
   </ns0:InputDocuments>

   <ns0:OutputDocuments>
      <!--Documento enviado na solicitação adicional, com os dados para a realização do
pagamento-->
      <ns0:OutputDocument DocId="DadosPagamento"
                          FriendlyName="Dados para realizar o pagamento"
                          DocURI="http://Banco/Docs/DadosPagamento">
         <ns0:SolicitacaoAdicional/>
         <ns0:MandatoryDocAttributes>
            <ns0:MandatoryDocAttribute MdaId="DP-Entidade"
                                       FriendlyName="Entidade para pagamento"
                                       AggregationAttr="true"
                                       AggUnitRef="EntPagamento" >
               <ns0:XPathExpr>//*[@AttId='Entidade']</ns0:XPathExpr>
            </ns0:MandatoryDocAttribute>
            <ns0:MandatoryDocAttribute MdaId="DP-Referencia"
                                       FriendlyName="Referencia para pagamento"
                                       AggregationAttr="true"
                                       AggUnitRef="RefPagamento" >
               <ns0:XPathExpr>//*[@AttId='Referencia']</ns0:XPathExpr>
            </ns0:MandatoryDocAttribute>
            <ns0:MandatoryDocAttribute MdaId="Valor"
                                       FriendlyName="Valor para pagamento"
                                       AggregationAttr="false" >
               <ns0:XPathExpr>//*[@AttId='Valor']</ns0:XPathExpr>
            </ns0:MandatoryDocAttribute>
         </ns0:MandatoryDocAttributes>
      </ns0:OutputDocument>
      <!--Resultado final da execução do serviço-->
      <ns0:OutputDocument DocId="ComprovativoPagamentoIMT"
                          FriendlyName="Comprovativo de pagamento do IMT"
                          DocURI="http://financas.pt/docs/CPagamentoIMT">
         <ns0:MandatoryDocAttributes>
         </ns0:MandatoryDocAttributes>
      </ns0:OutputDocument>
   </ns0:OutputDocuments>

   <ns0:AggregationDefinition>
      <ns0:AggregationUnit AggId="NSS"
                           FriendlyName="Número da Segurança Social"
                           ToObfuscate="true">
         <ns0:Description>
Agregar documentos com base no Número da Segurança Social</ns0:Description>
         <ns0:Obfuscation Algorithm="AES/CFB8/NoPadding" Encoding="Base64"/>
      </ns0:AggregationUnit>
      <ns0:AggregationUnit AggId="EntPagamento"
                           FriendlyName="Entidade para receber o pagamento"
                           ToObfuscate="false">
         <ns0:Description>
```

```
Verificar se a entidade no comprovativo de pagamento coincide com a entidade no
documento com os dados para pagamento.</ns0:Description>
      </ns0:AggregationUnit>
      <ns0:AggregationUnit AggId="RefPagamento"
                           FriendlyName="Referência para pagamento" ToObfuscate="false">
         <ns0:Description>
Verificar se a referência no comprovativo de pagamento coincide com a referencia no
documento com os dados para pagamento.</ns0:Description>
      </ns0:AggregationUnit>
   </ns0:AggregationDefinition>
</ns0:Documents>
```

4.3.3.4 Definição de Circunstâncias

Nos casos em que a entrega de determinados documentos pelos cidadãos esteja dependente de alguma circunstância destes, a RDP deve especificar essas circunstâncias e quais as regras de decisão que, com base nessas circunstâncias, determinam quais os documentos que um cidadão específico deve entregar para poder obter o serviço.

Considerámos que para cada circunstância existe apenas um número limitado de situações, todas elas previamente conhecidas. Por exemplo, no cenário considerado, a necessidade da apresentação do documento **Minuta do Banco** depende apenas de o cidadão ter ou não pedido um empréstimo para financiar a compra da casa, não existindo nenhuma outra possibilidade. Assim, considerámos que a inquirição das circunstâncias do cidadão pode ser feita através da apresentação de um conjunto de possíveis respostas, devendo o cidadão selecionar uma delas, não sendo necessárias formas mais complexas de introdução de dados. Além disso, desta forma as regras de decisão podem ser definidas apenas com recurso a igualdades, não sendo necessária a utilização de expressões lógicas mais complexas.

Apesar de a regra de decisão existente no cenário de exploração ser simples, envolve apenas uma decisão com base numa expressão contendo uma igualdade, na definição da RDP considerámos a possibilidade de existência de regras de decisão mais complexas, envolvendo múltiplas decisões encadeadas, como as ilustradas no excerto de pseudo-código que apresentamos no Excerto 5.

Excerto 5 Algoritmo que ilustra as regras de decisão que podem ser especificadas numa RDP.

```
if(expression)
then{
   if(expression)
   then {…}
```

```
   else{}
}
else {
   if(expression)
   then {…}
   else{}
}
```

As expressões consideradas são expressões lógicas (i.e., que produzem um resultado booleano) e envolvendo operadores relacionais e lógicos.

O Excerto 6 ilustra a definição de circunstâncias e regras de decisão na RDP do serviço *Pedido de Registos Provisórios*, em que o cidadão apenas precisa de apresentar a **Minuta do Banco** se tiver recorrido a um empréstimo para a compra da casa.

Excerto 6 Especificação de circunstâncias do cidadão e de regras de decisão, na RDP do serviço Pagamento do IMT.

```
    <ns0:Circumstances>
        <ns0:Circumstance CircId="Emprestimo"
                          CircType="CitizenCircumstance" DataType="String">
            <ns0:Question>
Recorreu a um empréstimo bancário para a compra da casa?</ns0:Question>
            <ns0:Answers>
                <ns0:Answer Position="0">
                    <ns0:Text>Sim</ns0:Text>
                </ns0:Answer>
                <ns0:Answer Position="1">
                    <ns0:Text>Não</ns0:Text>
                </ns0:Answer>
            </ns0:Answers>
        </ns0:Circumstance>
    </ns0:Circumstances>
    <ns0:DecisionRule>
        <ns0:BooleanExpression>
            <ns0:LeftOperand Type="Circumstance">
                <ns0:OpCircumstance CircRef="Emprestimo"></ns0:OpCircumstance>
            </ns0:LeftOperand>
            <ns0:Operator Name="Equal"></ns0:Operator>
            <ns0:RightOperand Type="Literal">
                <ns0:OpLiteral DataType="String">Sim</ns0:OpLiteral>
            </ns0:RightOperand>
        </ns0:BooleanExpression>
        <ns0:CaseTrue>
            <ns0:RequiredDocs>
                <ns0:RequiredDoc DocRef="CRP-PRP-CPredial-In-01"></ns0:RequiredDoc>
                <ns0:RequiredDoc DocRef="CRP-PRP-MinutaBanco-In-02"></ns0:RequiredDoc>
                <ns0:RequiredDoc DocRef="CRP-PRP-Mod1-In-03"></ns0:RequiredDoc>
                <ns0:RequiredDoc DocRef="CRP-PRP-CPCV-In-04"></ns0:RequiredDoc>
                <ns0:RequiredDoc DocRef="CRP-PRP-AId-In-05"></ns0:RequiredDoc>
```

```
            <ns0:RequiredDoc DocRef="CRP-PRP-CPagamento-In-06"></ns0:RequiredDoc>
        </ns0:RequiredDocs>
    </ns0:CaseTrue>
    <ns0:CaseFalse>
        <ns0:RequiredDocs>
            <ns0:RequiredDoc DocRef="CRP-PRP-CPredial-In-01"></ns0:RequiredDoc>
            <ns0:RequiredDoc DocRef="CRP-PRP-Mod1-In-03"></ns0:RequiredDoc>
            <ns0:RequiredDoc DocRef="CRP-PRP-CPCV-In-04"></ns0:RequiredDoc>
            <ns0:RequiredDoc DocRef="CRP-PRP-AId-In-05"></ns0:RequiredDoc>
            <ns0:RequiredDoc DocRef="CRP-PRP-CPagamento-In-06"></ns0:RequiredDoc>
        </ns0:RequiredDocs>
    </ns0:CaseFalse>
</ns0:DecisionRule>
```

4.3.3.5 Assinatura Digital

Uma RDP deve ser sempre assinada digitalmente, para garantir a sua integridade e a sua proveniência. Em termos do protótipo, as RDP são assinadas digitalmente, de acordo com a norma *XML Signature* (Bartel et al. 2008), com uma assinatura do tipo *Enveloped Signature*, contida na própria RDP, e incluindo o certificado para a validação da assinatura.

4.3.4 CHAPPIE

Quanto ao protótipo do Chappie, trata-se de um cliente dinâmico de *Web Services*, i.e., de uma aplicação que não conhece à partida o WSDL do *Web Service* que vai obter. Implementa as seguintes funcionalidades:

- Construir a árvore de dependências com base nas RDP que obtém a partir de um serviço raiz que lhe é indicado;
- Interagir com o cidadão para obter dados necessários para a construção da árvore de dependências (circunstâncias e localização de serviços que podem ser prestados por múltiplas IPS) e para a obtenção do serviço (dados pedidos pelos serviços e documentos a produzir pelo cidadão);
- Apresentar ao cidadão a árvore de dependências e permitir a análise dos pedidos de documentos de cada serviço;
- Obter os vários serviços que compõem a árvore de dependências; e

- Apresentar ao cidadão todo o serviço OEV obtido e permitindo-lhe observar os documentos obtidos.

A interface do Chappie é uma interface simples, concebida apenas para funcionar como prova de conceito, pelo que não inclui funcionalidades que são importantes como, por exemplo, permitir o acompanhando individual da obtenção de cada serviço e possibilitar a análise dos documentos obtidos de um serviço antes de prosseguir para a obtenção do seguinte.

Em termos da obtenção dos serviços, não foi feita qualquer paralelização nem otimização da sequência de obtenção, sendo estes obtidos seguindo um varrimento pós-ordem da árvore de dependências, começando por um serviço numa das extremidades (folhas) até terminar no Serviço Raiz.

4.4 EXPLORAÇÃO DO PROTÓTIPO

Implementado o protótipo, demos início à análise da obtenção do serviço OEV para a compra de casa. A obtenção do serviço OEV tem início com a introdução do endereço do serviço Raiz, que no caso do cenário exploratório é o serviço *Submissão de Documentos para Escritura Pública*. Na Figura 21 apresenta-se o ecrã do Chappie com o endereço do serviço Raiz introduzido.

A partir daqui dá-se início ao processo de construção da árvore de dependências, que decorre de forma automática com exceção de interrupções para lidar com circunstâncias, ilustrado na Figura 22, e, nos casos de documentos passíveis de ser obtidos de várias instituições, para o cidadão indicar qual o endereço do serviço a usar, o que está ilustrado na Figura 23.

Nesta última situação, em que o serviço a selecionar pode ser de um determinado tipo, o Chappie permite a seleção de um de entre os vários que o cidadão tenha anteriormente indicado, como se ilustra na Figura 23, onde se mostram dois bancos que podem fornecer o serviço pretendido, devendo o cidadão selecionar um deles.

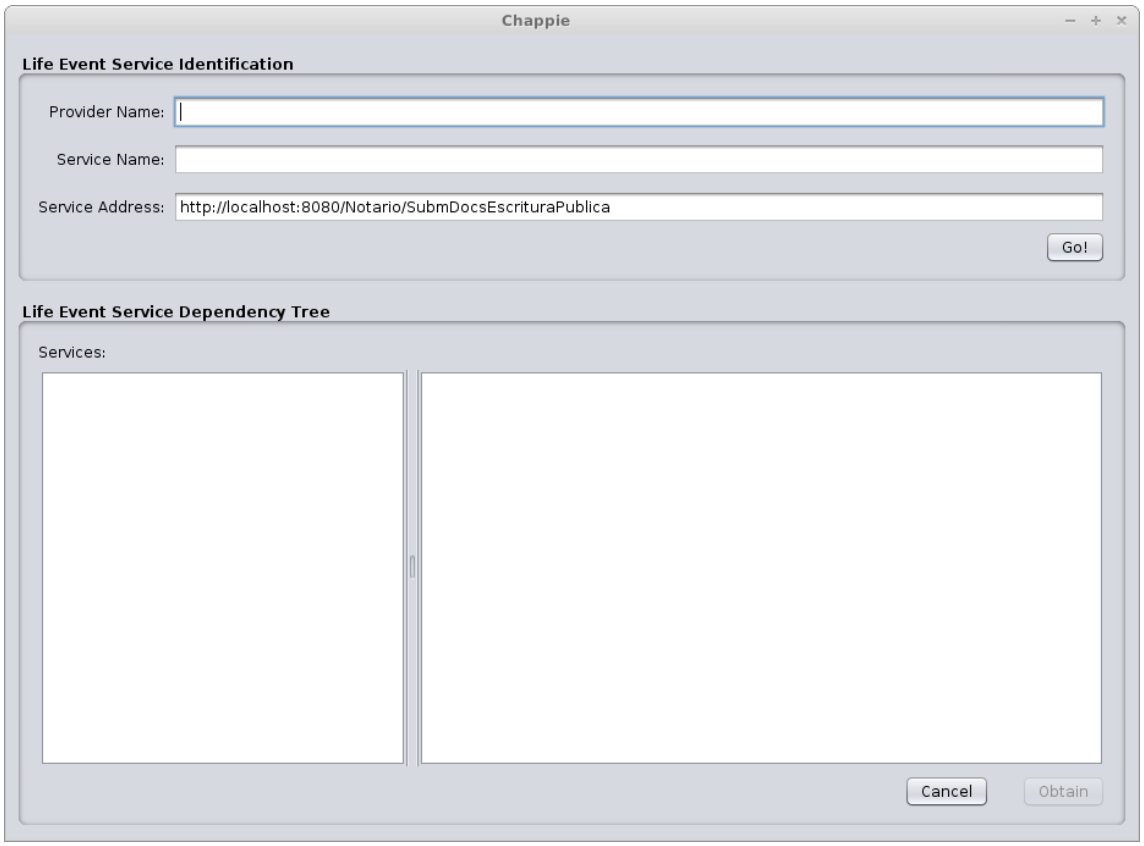

Figura 21: Ecrã do Chappie no início de obtenção de um serviço OEV, apenas com o endereço do serviço Raiz a partir do qual dará início ao processo de construção da árvore de dependências.

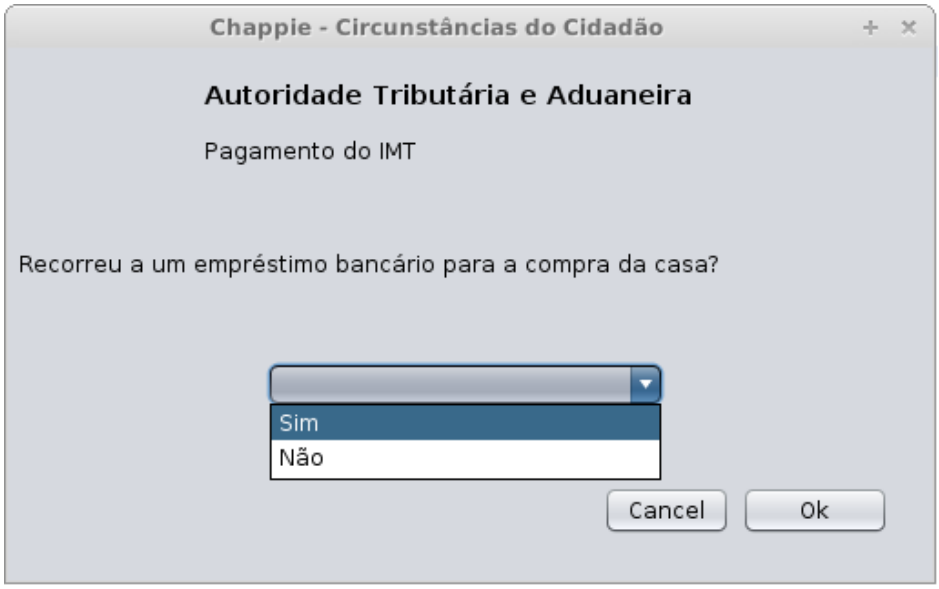

Figura 22: Ecrã do Chappie para o cidadão indicar as suas circunstâncias.

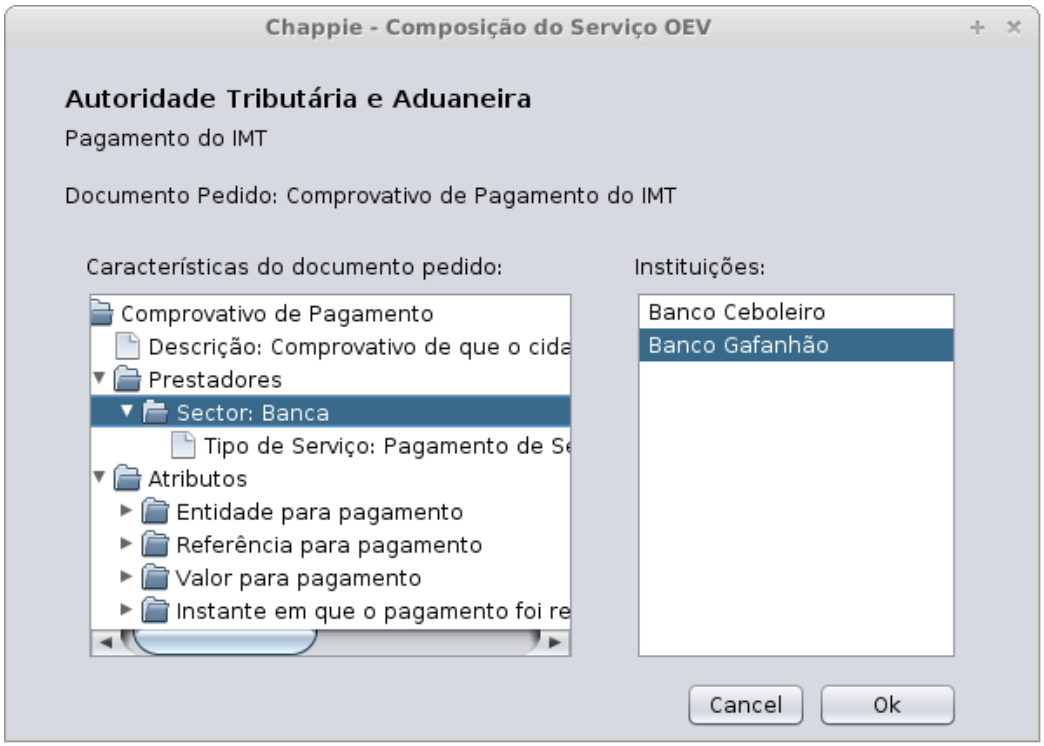

Figura 23: Ecrã do Chappie para permitir que o cidadão indique qual a instituição onde se deve ir obter um serviço de determinado tipo.

Depois de concluída a construção da árvore de dependências, ela é apresentada no ecrã do Chappie para que o cidadão a possa analisar. Nomeadamente, o cidadão pode verificar quais são os serviços que é necessário adquirir e toda a informação relativa a cada um deles, tal como:

- A instituição que o fornece;
- Quais os documentos que o serviço pede e emite;
- Os atributos que devem constar em cada um dos documentos e, destes, quais os que são usados para a agregação de documentos e, destes últimos, quais são para ofuscar;
- Quais os documentos que o cidadão tem de produzir e fornecer; e
- Quais os dados que o serviço pede para o cidadão introduzir diretamente.

Na Figura 24 apresenta-se um ecrã onde são visíveis, do lado esquerdo do ecrã, todos os serviços parciais que compõem a árvore de dependências do serviço OEV *Compra de Casa*. Na parte direita são apresentadas as características do serviço selecionado, que

no caso concreto é o serviço *Pagamento do IMT*, onde podemos observar um dos documentos pedidos pelo serviço, a Declaração de Situação Contributiva, e observar ainda que esse documento tem três atributos (na parte visível do ecrã). Podemos observar as características de um desses atributos, o Número de Identificação da Segurança Social (NISS), que é um atributo de agregação e que deve ser ofuscado usando o algoritmo AES, no modo de cifra CFB8, sem utilização de *padding* (*no padding*) e codificado em Base64.

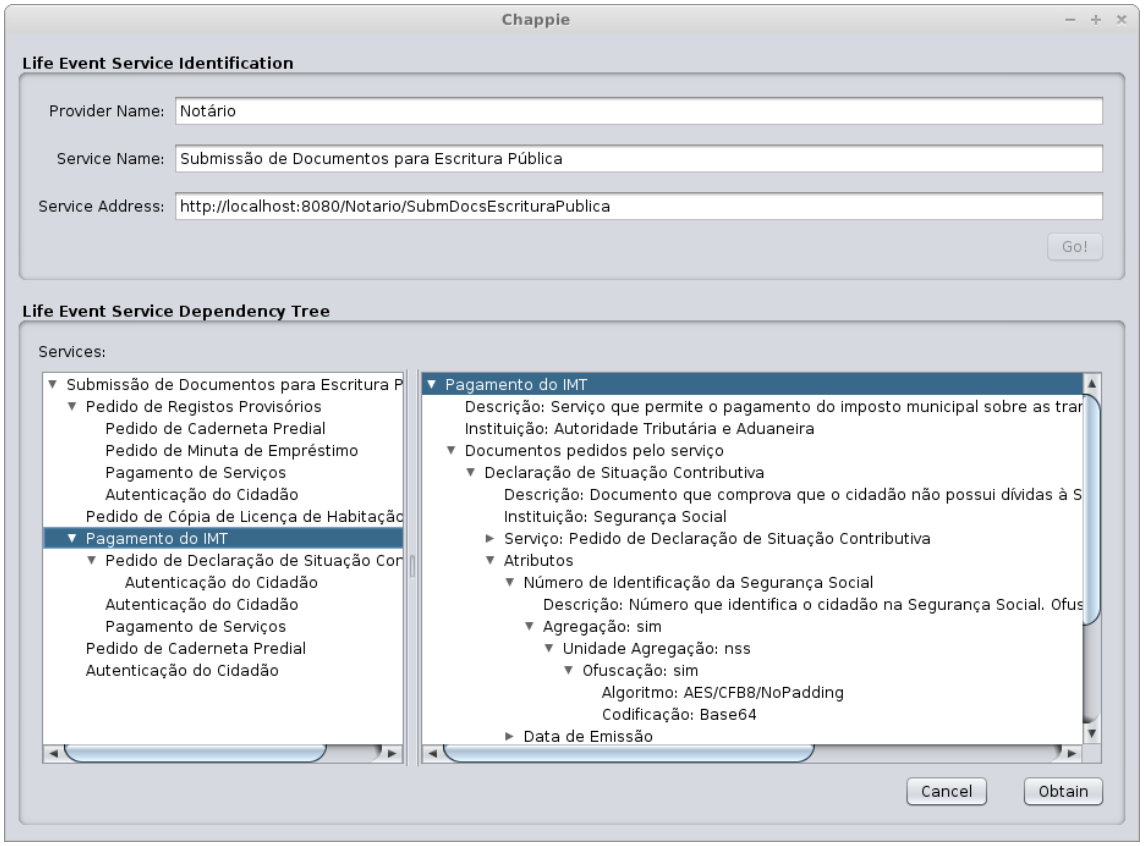

Figura 24: Ecrã do Chappie com a árvore de dependências do serviço OEV *Compra de Casa*.

Este ecrã com a árvore de dependências é fundamental para que o cidadão conheça o serviço que pretende obter. No protótipo ele é rudimentar, não disponibilizando grandes funcionalidades, mas poderão ser adicionadas mais funcionalidades como, por exemplo: permitir a alteração de serviços por outros que produzam os mesmos documentos; ou permitir que o cidadão indique que já possui um documento, pelo que não é necessário obter o serviço que o emite; ou obter dados previamente armazenados que sejam pedidos pelos serviços, etc.

Depois de ter analisado o serviço OEV, o cidadão pode dar início à sua obtenção, que consiste na obtenção sucessiva de cada um dos serviços parciais presentes na árvore

dependências. Esta obtenção decorre de forma automática, com interrupções sempre que o cidadão tenha de introduzir dados necessários para poder obter um serviço, como ilustrado na Figura 25 para a obtenção do serviço *Pedido de Cópia de Licença de Habitação*, onde é pedido ao cidadão para introduzir os dados que identificam a casa pretendida.

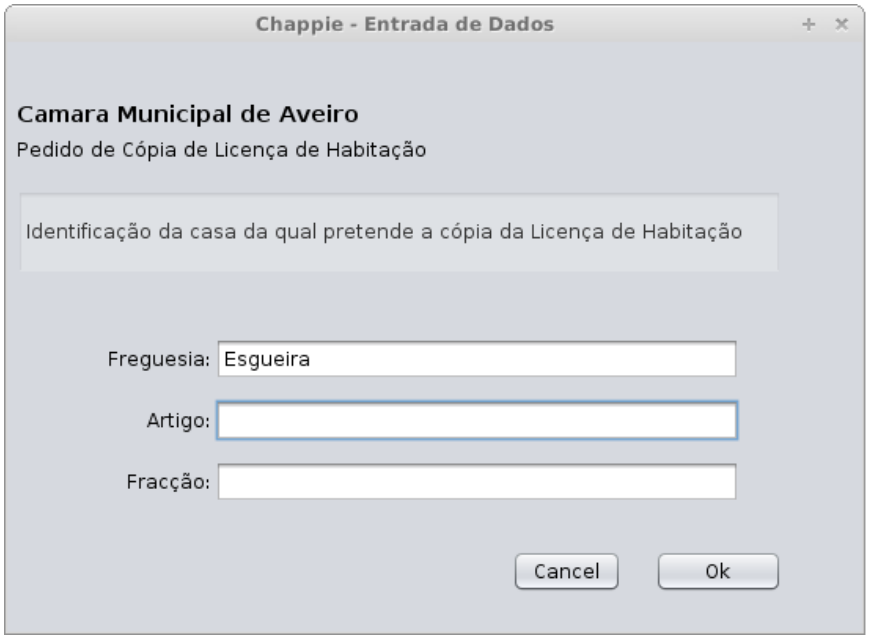

Figura 25: Ecrã do Chappie para que o cidadão introduza dados necessários para a prestação de um serviço. No caso concreto para a obtenção da cópia de uma Licença de Habitação.

No final da obtenção do serviço OEV, apresenta-se ao cidadão um ecrã onde ele pode analisar todos os documentos e demais informação sobre o serviço obtido. Este ecrã é semelhante ao ecrã com a árvore de dependências, só que agora está acrescentado com informação sobre cada um dos serviços obtidos. Podemos ver na Figura 26 um exemplo deste ecrã, onde se podem observar os valores de dois atributos, o Número de Identificação Fiscal do comprador e do vendedor da casa, no documento **Comprovativo de Pagamento de IMT**, produzido pelo serviço *Pagamento do IMT*. Reparar que também se permite a visualização completa dos documentos (clicando na linha que diz: "Clique para visualizar o documento") através da invocação da aplicação externa que lida com o tipo de ficheiro obtido.

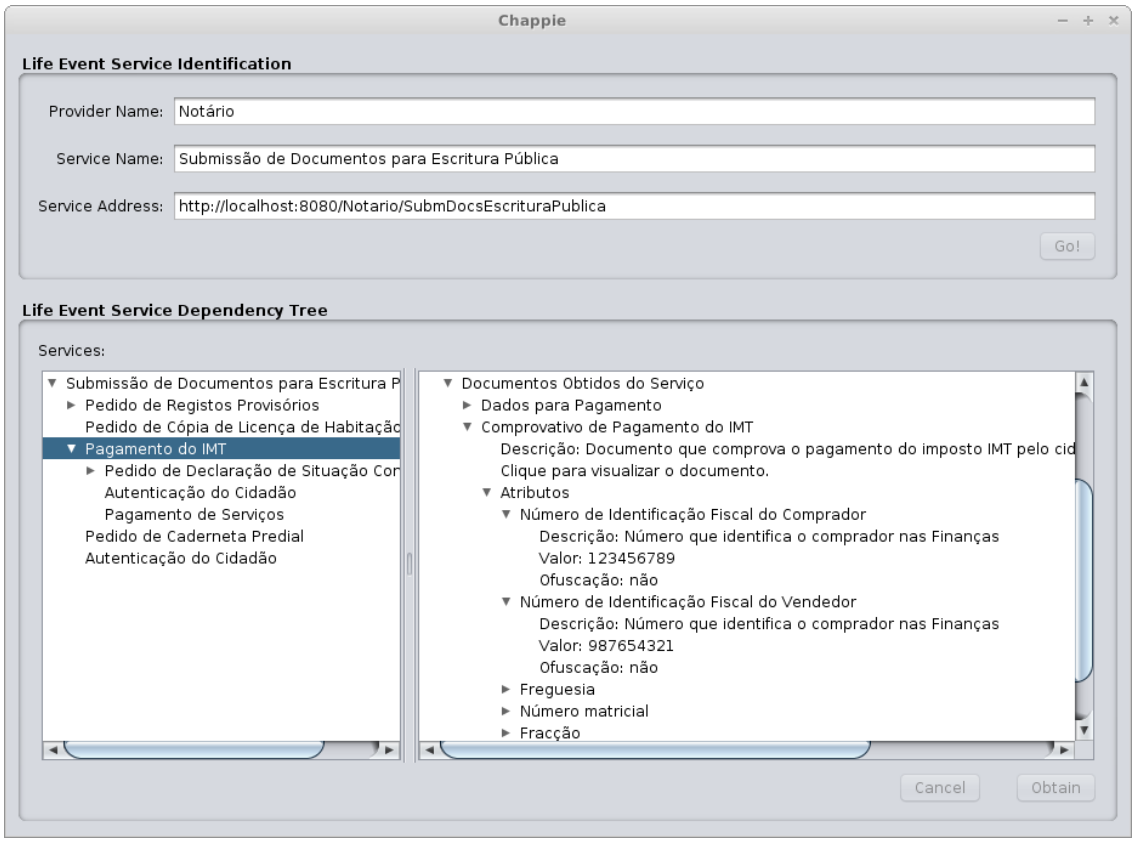

Figura 26: Exemplo de ecrã do Chappie onde o cidadão pode analisar toda a informação referente a um serviço OEV obtido.

Na Figura 27 apresentamos um outro exemplo do ecrã com o resultado da obtenção do serviço OEV, onde podemos observar alguns detalhes do documento **Declaração de Situação Contributiva**, que foi fornecido ao serviço *Pagamento do IMT* e produzido pelo serviço *Pedido de Declaração de Situação Contributiva*, e onde podemos ver o atributo NISS ofuscado, tal como era pedido pelo serviço *Pagamento do IMT*.

4.5 Discussão

Nesta secção vamos discutir alguns aspetos referentes à prova de conceito realizada.

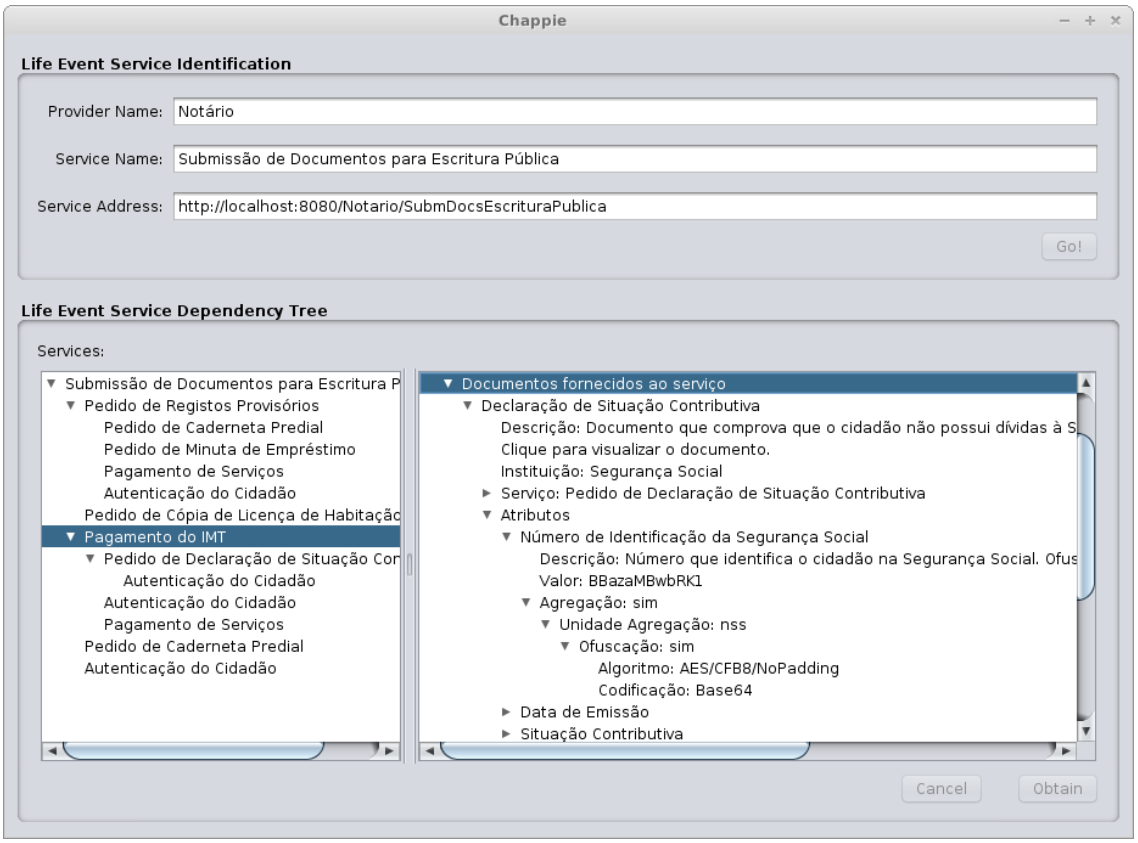

Figura 27: Outro exemplo de ecrã do Chappie onde o cidadão pode analisar toda a informação referente a um serviço OEV obtido e onde se pode observar um atributo ofuscado.

Tendo em conta os três objetivos definidos para a prova de conceito, concluímos da exploração do cenário de compra de casa que o modelo CHAPAS se adequa à obtenção de serviços OEV pelo cidadão, ainda que com algumas limitações. Com efeito:

- O Chappie permitiu construir a árvore de dependências completa para o serviço OEV, com base nas RDP dos vários serviços que fornecem os documentos necessários para que o cidadão possa obter o Serviço Raiz que marca a obtenção completa do serviço OEV;
- O Chappie permitiu também obter os vários serviços que compõem a árvore de dependências; e
- Foi realizada a agregação de documentos com base em atributos ofuscados.

No entanto, apesar de termos verificado os objetivos, verificámos algumas limitações que apontamos de seguida.

Uma delas prende-se com os documentos produzidos pelo cidadão, que não são tratados pelo Chappie da mesma forma que os documentos trocados entre instituições. Nomeadamente, o Chappie não é capaz de verificar atributos no seu interior. Isto poderia ser possível se os documentos produzidos pelo cidadão tivessem como base algum formulário suportado num esquema de documento que permita a navegação no documento. Isto pode ser realizado, por exemplo com formulários baseados em Microsoft Word, mas implica que o Chappie venha a lidar com formatos específicos de documentos, tal como já faz com o XML.

Uma outra prende-se com a agnosticidade do Chappie em relação ao conteúdo dos documentos. Esta agnosticidade permite que o Chappie não fique dependente dos conteúdos dos documentos que por ele circulam nem dos serviços onde os obtém, desde que estes mantenham as respetivas RDP atualizadas e acessíveis. No entanto, também pode criar algumas limitações nas funcionalidades do Chappie, nomeadamente em relação à exploração e utilização da informação. Por exemplo, para obter a Caderneta Predial e a Cópia da Licença de Habitação, o cidadão tem de introduzir a identificação do imóvel que pretende adquirir em cada um dos respetivos serviços. Uma outra situação ocorre com a obtenção do serviço *Pedido de Caderneta Predial*, que é obtido duas vezes, uma vez que a **Caderneta Predial** é pedida pelo serviço Raiz, *Submissão de Documentos para Escritura Pública*, e pelo serviço *Pedido de Registos Provisórios*. Também o serviço Pagamento de Serviços é obtido duas vezes, para realizar dois pagamentos, mas aqui claramente não há uma repetição de serviços porque se trata de dois pagamentos distintos. Nestas situações, devido à sua agnosticidade, o Chappie não tem possibilidade de decidir se se trata ou não de obtenções repetidas, pelo que a regra é obter sempre. Este mesmo problema também impede a reutilização de documentos já na posse do cidadão, uma vez que o Chappie não tem possibilidade de determinar se um documento na posse do cidadão corresponde a algum documento pedido por um serviço. A quebra da agnosticidade do Chappie, com a utilização de ontologias da AP, tanto pelo Chappie como pelas várias instituições, poderia ser uma forma de resolver este problema.

Há também a questão das falhas, que podem ocorrer por múltiplas razões, desde enganos na introdução de dados pelo cidadão, a informação em falta nos documentos, etc. No cenário de exploração apenas se lidou com falhas devido a enganos nos dados introduzidos pelo cidadão, sendo a solução para este caso a geração de um erro que provoca o refazer do pedido e a consequente reintrodução dos dados. No entanto, este assunto deve ser alvo de uma melhor análise, em conjunto com as IPS, para permitir que o

cidadão tenha um canal de fácil acesso para tratar as falhas que ocorram na obtenção dos serviços.

Quanto à autenticação explícita do cidadão usando o seu Cartão de Cidadão, ela não se revelou um problema pelo facto de, com esse cartão, o PIN ser solicitado uma única vez para a realização de múltiplas assinaturas (usando a chave privada de autenticação) por uma mesma instância de um programa em execução. Assim, o cidadão não tem de introduzir o seu PIN por cada serviço que seja obtido no contexto de um serviço OEV. No entanto, isto não invalida a necessidade de estudos adicionais para a incorporação de mecanismos e protocolos de autenticação no modelo CHAPAS.

Uma questão pertinente que pode emergir desta validação é se a adequação do modelo CHAPAS para a obtenção do serviço OEV *Compra de Casa* se pode estender à generalidade dos serviços OEV ou apenas a um subconjunto mais ou menos reduzido/alargado destes. Claramente, a obtenção de serviços OEV no modelo CHAPAS está limitada por este não incluir os serviços parciais do tipo Complementar (*After Care*). Isto verifica-se mesmo para o cenário explorado, em que não se consideraram os serviços complementares *Pedido de Isenção de IMI* e *Conversão dos Registos Provisórios em Definitivos*. A razão para esta exclusão é o facto de eles não se enquadrarem na modelação por árvores de dependências, porque eles não contribuem para o serviço Raiz, uma vez que a sua obtenção apenas pode ocorrer posteriormente. Este é um assunto a resolver em trabalho futuro.

Por outro lado, como a obtenção de serviços OEV no modelo CHAPAS parte sempre de um serviço Raiz, os serviços OEV em que não seja possível identificar um serviço Raiz poderão não se adequar diretamente a ser obtidos no modelo CHAPAS. Estes serviços foram identificados como a exceção ao modelo de referência de serviços OEV genéricos (Todorovski et al. 2007) em que o CHAPAS se baseia, apresentado na secção 2.1.5.3, e caracterizam-se por a definição dos serviços Cruciais a obter estar dependente dos interesses do cidadão. Por exemplo, num serviço OEV *Perdi a Minha Carteira*, a definição dos serviços Cruciais depende dos documentos em concreto que o cidadão perdeu, não sendo possível identificar um serviço Crucial para ser o serviço Raiz no modelo CHAPAS. No entanto, este tipo de serviços OEV poderá ser adaptado ao modelo CHAPAS com a introdução de um serviço Raiz fictício, com o único objetivo de disponibilizar uma RDP para transformar em serviços de Suporte os serviços Cruciais cuja obtenção depende de interesses do cidadão, usando circunstâncias para expressar esses interesses do cidadão.

4.6 RESUMO

Neste capítulo fizemos a prova do conceito do modelo CHAPAS, tendo como base um cenário de exploração para o evento de vida compra de casa e um protótipo que implementámos. Desta exploração concluímos que, com algumas limitações, é viável a utilização do modelo CHAPAS para a obtenção de serviços OEV, ainda que não seja possível a sua utilização na totalidade dos serviços OEV, mas que pode ser potenciado se se dotar o Chappie com a capacidade de lidar com formatos específicos de ficheiros, se o modelo incorporar ontologias que venham a ser desenvolvidas e adaptadas pela AP e se forem criados canais alternativos para facilitar a comunicação do cidadão com as IPS para tratar de eventuais falhas na obtenção dos serviços.

5 CONCLUSÕES

Ao longo dos anteriores quatro capítulos apresentámos a motivação, o problema, os objetivos e as contribuições deste trabalho de tese; fizemos também uma contextualização do trabalho em conjunto com a apresentação do trabalho relacionado, na qual apresentámos uma panorâmica da evolução da prestação de serviços de governo eletrónico ao cidadão, um conjunto de conceitos sobre a identificação dos cidadãos, o conceito de Arquitetura Orientada a Serviços (SOA) e um conjunto de aplicações e tecnologias que podem colocar do lado do utilizador (em dispositivos controlados por este) o controlo da informação deste; apresentámos o modelo CHAPAS, o modelo que propomos para a prestação de serviços OEV, que devolve ao cidadão, assistido pelo seu Chappie, um papel ativo na obtenção dos vários serviços que compõem o serviço OEV e o coloca (ao cidadão) no centro do fluxo de informação necessária para a prestação dos serviços por ele pretendidos; apresentámos a prova de conceito, que envolveu a definição de um cenário de exploração com base no evento da vida de compra de casa, o desenvolvimento de um protótipo do Chappie e dos serviços prestados pelas várias instituições e, por fim, exploração do cenário usando os protótipos, o que nos permitiu validar o modelo.

Neste capítulo, concluímos a tese com a apresentação de uma panorâmica sobre o trabalho realizado e com a indicação de possíveis caminhos para trabalho futuro.

5.1 PANORÂMICA SOBRE O TRABALHO REALIZADO

Neste trabalho de tese propusemos um novo modelo para a prestação de serviços OEV ao cidadão, o modelo CHAPAS.

Os serviços OEV são serviços complexos que visam atender a situações concretas que os cidadãos sentem no seu dia-a-dia e cuja satisfação normalmente envolve a obtenção pelo cidadão de vários serviços, possivelmente prestados por várias instituições, públicas e/ou privadas. Assim, um elemento fundamental na prestação eletrónica deste tipo de serviços é o controlo sobre o fluxo de informação entre as várias instituições envolvidas.

Inicialmente a informação do cidadão estava compartimentada em silos, i.e., em instituições autónomas que prestavam serviços ao cidadão tipicamente com base nas suas competências. A comunicação direta entre estas instituições era reduzida, pelo que era da responsabilidade do cidadão o fornecimento de toda a informação externa (na posse de outras instituições) necessária para a prestação de um serviço pretendido. O cidadão era o veículo de comunicação entre instituições, para efeito da prestação dos serviços por ele pretendidos, tendo por isso controlo sobre a difusão da sua informação entre as várias instituições. Ou seja, apesar de algumas desvantagens, este modelo era amigo da privacidade do cidadão porque dificultava uma visão global da informação do cidadão na posse da AP, no seu todo, e permitia que o cidadão tivesse noção da informação que cada instituição possuía sobre si.

Com a progressiva integração da AP, com o objetivo de prestar serviços mais cómodos e orientados às necessidades do cidadão, as instituições começaram a trocar informação entre si retirando ao cidadão o papel de veículo de comunicação entre as instituições. Com isto, o cidadão perde o controlo sobre o fluxo da sua informação entre instituições, uma vez que deixa de ter a perceção direta de quais as instituições envolvidas na troca de informações e de qual a informação trocada entre elas, além de que passa a existir o potencial para uma fácil agregação de toda a informação do cidadão na posse da AP.

O objetivo deste trabalho foi o de conciliar os benefícios para a privacidade do cidadão potenciados pela organização da AP em silos com os benefícios da prestação de melhores serviços potenciados pela integração da AP, como é o caso da prestação de serviços orientados a eventos da vida. Na prossecução deste objetivo, a contribuição central desta tese é o modelo CHAPAS (*Citizen-side HAndling of Public Administration e-Services*), que foi apresentado e discutido no capítulo 3.

Neste trabalho questiona-se o modelo atual de prestação de serviços ao cidadão e o pensamento dominante, de que a prestação de melhores serviços implica a progressiva integração entre instituições. Abrimos também novas perspetivas para a prestação de

serviços ao cidadão, ao demonstrar que é possível prestar serviços complexos sem que as várias instituições participantes comuniquem diretamente entre si, ou seja, mantendo a independência entre instituições e mantendo no cidadão o papel de difusor da sua informação. Não se pretende de forma alguma impedir que as instituições comuniquem diretamente entre si, até porque essa comunicação é fundamental para muitos aspetos do seu dia-a-dia, mas apenas demonstrar que, para o caso concreto da prestação de serviços ao cidadão, existem alternativas a esta comunicação direta, com a vantagem de que mantêm no cidadão algum controlo sobre a difusão da sua informação, o que é importante para a confiança deste nas práticas das instituições.

São então as seguintes as principais características do modelo CHAPAS:

- Recoloca o cidadão no controlo do fluxo da sua informação entre instituições, auxiliado pelo seu Chappie, uma ferramenta que é executada num dispositivo do cidadão e que o auxilia na obtenção dos vários serviços e lhe permite controlar a informação que flui entre serviços;
- A publicação pelas instituições de uma política (RDP – *Required Documents Policy*) para cada um dos seus serviços, em que definem toda a informação relevante para que o cidadão possa obter o respetivo serviço, o que inclui a identificação dos documentos a entregar, eventualmente tendo em consideração circunstâncias dos cidadãos;
- A composição semiautomática de serviços OEV, envolvendo múltiplas instituições, de acordo com um modelo em árvore de dependências, realizada pelo cidadão no seu Chappie e guiada pelas indicações nas RDP dos vários serviços;
- A disponibilização de mecanismos que permitem a minimização do fluxo de informação entre instituições (mediado pelo cidadão) para o mínimo estritamente necessário para a prestação dos serviços pretendidos.
- Ainda no contexto da minimização da informação, a disponibilização de um mecanismo (para o qual obtivemos uma patente nacional) que permite que as instituições agreguem documentos com base em atributos ofuscados sob controlo do cidadão, i.e., a agregação de documentos sem a revelação dos valores dos identificadores comuns nesses documentos.

Para a validação do modelo proposto foi feita uma prova de conceito que envolveu a definição de um cenário de exploração baseado no evento da vida *compra de casa* e a construção de protótipos para o Chappie e para os serviços prestados pelas várias instituições. A escolha deste evento da vida, a compra de casa, deveu-se ao facto de ele ser complexo, envolvendo oito serviços prestados por cinco instituições da AP e uma instituição privada, e de ser uma situação pela qual muitos dos cidadãos passam ao longo da sua vida. Na implementação do protótipo, os serviços prestados pelas várias instituições foram implementados como *Web Services*, sendo o Chappie uma aplicação cliente desses *Web Services*. Além disso, foi necessário desenvolver uma sintaxe para permitir às várias instituições exprimir os requisitos que cada serviço coloca para a sua obtenção, i.e., para implementar a sua RDP.

A exploração do cenário, usando os protótipos, permitiu-nos concluir que o modelo CHAPAS cumpre o objetivo a que se propunha, uma vez que permite que o cidadão obtenha serviços OEV complexos envolvendo múltiplas instituições, embora com algumas limitações, e mantendo o cidadão com veículo para o fluxo de informação entre instituições, o que lhe permite controlar a disseminação da sua informação pelas várias instituições.

5.1.1 PONTOS FORTES DO MODELO CHAPAS

Nesta secção apresentamos uma súmula dos pontos fortes que o modelo CHAPAS apresenta em relação à prestação integrada de serviços OEV.

Um ponto forte significativo é que o modelo CHAPAS devolve ao cidadão o controlo sobre a disseminação da sua informação pelas várias instituições da AP. Este controlo não é exercido através de mecanismos que impossibilitem a troca de informação entre instituições ou a utilização da informação para fins diversos daqueles para os quais o cidadão a forneceu, o que está sempre dependente da vontade de quem está na posse da informação. Este controlo é feito dotando o cidadão de mecanismos que lhe permitam saber, e registar, que informação forneceu a cada instituição, quando e em que contexto. Com este conhecimento, damos azo a que o cidadão possa estar consciente, documentado e alerta em relação à informação que fornece (ou forneceu) a cada instituição, o que lhe permite detetar eventuais abusos e excessos que coloquem em causa a sua privacidade, bem como fundamentar com dados concretos as eventuais iniciativas que tome com vista a denunciá-las.

Para proteger a privacidade do cidadão, é importante reduzir ao mínimo estritamente necessário a quantidade de informação que este tem de fornecer para poder obter os serviços. Assim, um outro ponto forte do modelo CHAPAS é que disponibiliza mecanismos que permitem às instituições minimizar a informação que pedem ao cidadão. Um destes mecanismos permite que as instituições indiquem de entre o conteúdo normal de um documento, quais os itens de informação (atributos) que pretendem receber, sendo os restantes omitidos do documento. O outro mecanismo, que foi objeto de uma patente no contexto desta tese, permite minimizar ainda mais a informação pedida pelas instituições, ao permitir fornecer de forma ofuscada os atributos cuja função é exclusivamente a agregação de documentos, sem que com isso deixem de cumprir a sua função.

Outro ponto forte do modelo CHAPAS é que a sua implantação não exige grandes esforços de remodelação nas instituições. Estas podem continuar a prestar os seus serviços nos mesmos moldes que prestavam anteriormente, sendo apenas necessário adaptar as interfaces destes serviços para funcionar de acordo com o modelo CHAPAS. Com efeito, a prestação de serviços no modelo CHAPAS não obriga à existência de reestruturações e de alinhamentos entre instituições, tal como acontece na prestação de serviços integrados, com todos os custos e dificuldades associados. Ou seja, a interoperabilidade organizacional tem pouco impacto no modelo CHAPAS, ao contrário do que acontece no modelo de prestação de serviços integrados.

Finalmente, um outro ponto forte do modelo CHAPAS é que ele potencia o envolvimento da comunidade no desenvolvimento de novas funcionalidades que possam trazer mais-valias para o cidadão com base na utilização da informação que resulta das suas interações com a AP. Isto decorre do facto de o Chappie ser uma aplicação do cidadão, que corre numa plataforma controlada por este, e que pode ser usada para a gestão da sua informação. Possibilitar o desenvolvimento de versões diferentes e concorrentes de Chappies pode ser importante para permitir, com custos reduzidos para o Estado, um contínuo rejuvenescimento da prestação de serviços ao cidadão.

5.1.2 PONTOS FRACOS DO MODELO CHAPAS

O modelo CHAPAS apresenta também um conjunto de pontos fracos em relação à prestação de serviços integrados.

Um ponto fraco é o tratamento de situações de falhas. Com efeito, as falhas surgem sempre e podem ter as mais variadas razões, algumas da responsabilidade do cidadão e outras da responsabilidade das instituições. No caso da prestação de serviços integrados, falhas que não estejam diretamente relacionadas com o cidadão, como falhas relacionadas com o fluxo de informação entre instituições, podem ser geridas pelas várias instituições sem que eventualmente o cidadão se aperceba da sua ocorrência. Já no modelo CHAPAS, todas as falhas acabam por ter alguma repercussão no cidadão, pelo que é fundamental que existam canais que facilitem ao cidadão a comunicação com as instituições para a resolução dos eventuais problemas que surjam devido à ocorrência de falhas.

Um outro ponto fraco tem a ver com o pagamento dos serviços OEV. Um serviço OEV caracteriza-se por envolver a participação de múltiplos serviços (serviços parciais) prestados por várias instituições. Cada um destes serviços pode ter um preço que a respetiva instituição prestadora deve receber. No modelo de prestação de serviços integrados, o serviço OEV é também controlado por uma instituição, que pode negociar acordos com as instituições que prestam os vários serviços parciais com vista à definição de preços e de condições de pagamento (interoperabilidade organizacional). Isto permite que o preço do serviço OEV seja apresentado ao cidadão como um preço único, que este deve pagar numa única vez, ficando a instituição que controla o serviço OEV com a responsabilidade de ressarcir as restantes instituições que nele participam.

Já no modelo CHAPAS, os serviços parciais são obtidos individualmente pelo cidadão, o que impede a existência de um pagamento único para todo um serviço OEV. Ou seja, como não há uma visão de conjunto do serviço OEV por parte das instituições, cada serviço terá de ser pago na altura da sua obtenção, o que implica múltiplos pagamentos no contexto da obtenção de um único serviço OEV. No entanto, isto também pode ser visto como um elemento adicional de controlo das instituições que participam no serviço OEV, uma vez que implica uma reforçada atenção do cidadão no papel de cada uma das instituições participantes.

5.2 TRABALHO FUTURO

O modelo CHAPAS é apenas uma visão, uma vez que está apenas "no papel", i.e., existe apenas como um protótipo laboratorial. Muitos aspetos existem para trabalhar no

sentido de eventualmente ele se poder transformar em realidade, alguns dos quais passamos a descrever:

- A incorporação de tecnologias que permitam a descoberta dos serviços, e respetivas instituições prestadoras, capazes de fornecer um determinado documento para que o cidadão possa escolher o mais adequado ao seu interesse. Esta funcionalidade é crucial para a composição dos serviços OEV porque auxilia o cidadão na identificação dos serviços que devem ser incluídos na árvore de dependências do serviço OEV pretendido.

- A incorporação de ontologias da AP para a definição de termos comuns a todas as partes. Esta incorporação é de particular interesse para o Chappie porque pode permitir facilitar os diálogos com o cidadão (o Chappie deixa de estar totalmente dependente da informação enviada pelo serviço) e pode permitir o surgimento de novas funcionalidades, com base na interpretação de conteúdos nos documentos, por exemplo.

- A inclusão dos serviços parciais Complementares no modelo CHAPAS. Estes serviços parciais apenas se obtêm como complemento a um serviço OEV previamente obtido, não sendo atualmente suportados pelo modelo CHAPAS, porque a sua incorporação num serviço OEV não se adapta à lógica da composição de serviços com base em árvores de dependência. No entanto, para uma melhor satisfação dos eventos da vida dos cidadãos, faz sentido a sua inclusão no modelo CHAPAS.

- A definição de uma PKI para o estabelecimento da confiança entre as várias instituições fornecedoras de serviços, o que é fundamental para a validação de assinaturas de documentos.

- A incorporação de tecnologias para a produção de documentos em XML de acordo com os esquemas definidos externamente (*custom* XML). Por exemplo, para que um Contrato Promessa de Compra e Venda seja produzido num documento com um formato XML próprio para esse efeito e não com um eventual formato XML específico do editor de texto usado pelo cidadão. Isto é de particular interesse para o Chappie para permitir que documentos produzidos pelo cidadão sejam tratados da mesma forma que os restantes documentos, o que atualmente não é possível.

- A incorporação de mecanismos e protocolos de autenticação para a autenticação do cidadão na obtenção dos vários serviços. A autenticação já foi superficialmente abordada neste trabalho, mas sem conclusões. Os aspetos importantes a ter em conta nesta incorporação são o garantir que os protocolos de autenticação não envolvam a comunicação direta entre instituições e que a interferência da autenticação do cidadão no processo de obtenção dos múltiplos serviços seja a menor possível.

- Um refinamento da sintaxe da RDP para que, sempre que possível, ela esteja de acordo com as múltiplas normas de *Web Services*, principalmente as referentes à definição de políticas.

- Estudo sobre a eventual adaptação do modelo CHAPAS a outros contextos e a tipos de clientes da AP, o que poderia ser interessante para promover a sua adoção.

- A disponibilização do Chappie como uma aplicação para dispositivos móveis é também uma área a investir dada a atual vulgarização das plataformas móveis.

- Um outro aspeto que poderá ser interessante é a convergência das funcionalidades de obtenção de serviços OEV com *Electronic Data Safes*, abordadas na secção 2.4.1, o que permitiria o desenvolvimento de soluções mais amplas para gestão e armazenamento da sua informação pessoal.

De um ponto de vista não técnico uma vertente de trabalho futuro importante é a sensibilização das instituições para a adesão ao modelo CHAPAS. Sem essa adesão o modelo nunca passará de protótipo laboratorial. Esta será a tarefa mais difícil de todas porque o modelo CHAPAS desvia-se do modelo de integração da AP que está atualmente em voga.

BIBLIOGRAFIA

Agência para a Modernização Administrativa, 2011. *INTEROPERABILIDADE NA ADMINISTRAÇÃO PÚBLICA: Procedimentos para a adesão à iAP - Plataforma de Interoperabilidae na Administração Pública*, AMA.

Al-Fedaghi, S.S. & Taha, M.M., 2006. Personal Information eWallet. In *2006 IEEE International Conference on Systems, Man, and Cybernetics*. Taipei, Taiwan, pp. 2855–2862.

Alves, A.A. & Moreira, J.M., 2005. *Cidadania Digital e Democratização Electrónica*, Porto: SPI - Sociedade Protuguesa de Inovação.

Arsanjani, A., Architect, C. & Group, S., 2004. Service-oriented modeling and architecture: How to identify, specify, and realize services for your SOA. *IBM DeveloperWorks*.

Assembleia da República, 2005. *Constituição da República Portuguesa (sétima revisão constitucional)*, http://ftp.infoeuropa.eurocid.pt/000038001-000039000/000038841.pdf.

Assembleia da República, 1998. Lei da Protecção de Dados Pessoais (67/98). *Diário da República - I Série-A*, pp.5536–5546.

Bannister, F., 2005. The Panoptic State: Privacy, Surveillance and the Balance of Risk. *Information Polity*, 10(1/2), pp.65–78.

Barhamgi, M. et al., 2011. Privacy-Preserving Data Mashup ∗. In *2011 International Conference on Advanced Information Networking and Applications*. IEEE Computer Society, pp. 467–474.

Bartel, M. et al., 2008. *XML Signature Syntax and Processing (Second Edition)*, W3C.

Bauer, D., 2009. Preserving privacy with user-controlled sharing of verified information. *Interface*, (December).

Baum, C., Di Maio, A. & Caldwell, F., 2000. What is e-government? Gartner definitions. *Research note TU-11-6474, Gartner Group*.

Bednar, P. et al., 2008. Semantic Integration of Government Services - the Access-eGov Approach. In P. Cunningham & M. Cunningham, eds. *Collaboration and the Knowledge Economy: Issues, Applications, Case Studies*. Amsterdan: IOS Press.

Belanger, F. & Hiller, J.S., 2006. A framework for e-government: privacy implications. *Business process management journal*, 12(1), pp.48–60.

Beldad, A. et al., 2012. A cue or two and I ' ll trust you : Determinants of trust in government organizations in terms of their processing and usage of citizens ' personal information disclosed online. *Government Information Quarterly*, 29(1), pp.41–49.

Beldad, A., Jong, M. De & Steehouder, M., 2011. I trust not therefore it must be risky: Determinants of the perceived risks of disclosing personal data for e-government transactions. *Computers in Human Behavior*, 27(6), pp.2233–2242.

Bellamy, C., 1999. Joining-Up Government in the UK: Towards Public Services for an Information Age. *Australian Journal of Public Administration*, 58(3), pp.89–96.

Benatallah, B. et al., 2005. Service Composition : Concepts, Technics, Tools and Trends. In *Service-oriented software system engineering: challenges and practices*. Idea Group Inc., pp. 48–66.

Benhaddi, M., Baina, K. & Abdelwahed, E.H., 2012. A user-centric Mashuped SOA. *Int. J. Web Science*, 1(3), pp.204–223.

Bennett, C.J., 2001. What Government Should Know about Privacy: A Foundation Paper. *Information Technology Executive Leadership Council's Privacy Conference*, 19.

Bennett, L., 2009. Reflections on privacy , identity and consent in on-line services. *Information Security Technical Report*, 14(3), pp.119–123.

Bergman, O. et al., 2004. Personal Information Management. In *CHI'04 extended abstracts on human factors in computing systems*. New York: ACM Press, pp. 1598–1599.

Berners-Lee, T., Hendler, J. & Lassila, O., 2001. The Semantic Web. *Scientific American*, 284(5), pp.34–43.

Bianchini, D., Antonellis, V. De & Melchiori, M., 2012. Towards Semantic-assisted Web Mashup generation. In *2012 23rd International Workshop on Database and Expert Sytems Applications*. IEEE, pp. 279–283.

Booth, D. et al. eds., 2004. *Web Services Architecture, W3C Working Group Note, 11 de Fevereiro de 2004*, World Wide Web Consortium (W3C).

Booth, D. & Liu, C.K., 2007. Web Services Description Language (WSDL) Version 2 . 0 Part 0 : Primer. *Style (DeKalb, IL)*, (June), pp.1–81.

Bray, T. et al. eds., 2006. *Extensible Markup Language (XML) 1.1 (Second Edition)*, W3C.

De Bri, F. & Bannister, F., 2010. Whole-of-government: The continuing problem of eliminating silos. In *Proceedings of the 10th European Conference on eGovernment, National Centre for Taxation Studies and University of Limerick, Ireland*. pp. 122–133.

Burr, W.E. et al., 2008. Electronic authentication guideline,. *NIST Special Publication 800-63-1*.

Burton, C., 2009. The Information Card Ecosystem: The Fundamental Leap from Cookies & Passwords to Cards & Selectors. *Information Card Foundation*.

Cameron, K., 2005. The laws of identity. *At http://www. identityblog.com/stories/2005/05/13/TheLawsOfIdentity. pdf*.

Camp, L.J., 2005. Digital identity. *IEEE Technology and Society Magazine*, 23(3), pp.34–41.

Cavoukian, A., 2006. 7 Laws of Identity: The case for privacy-embedded laws of identity in the digital age. *Technology*.

Cavoukian, A., 2013. Personal Data Ecosystem (PDE) - A Privacy by Design Approach to an Individual's Pursuit of Radical Control. In *Digital Enlightenment Yearbook 2013*. IOS Press, pp. 89–101.

Cavoukian, A., 2012. *Privacy by Design and the Emerging Personal Data Ecosystem*, Privacy By Design.

Christensen, E. et al., 2001. *Web Services Description Language (WSDL) 1.1*, W3C.

Christensen, T. & Laegreid, P., 2007. Th e Whole-of-Government Approach to Public Sector Reform. *Public Administration Review*, (November-December), pp.1059–1066.

Church, L. & Moloney, M., 2012. Public Value Provision : A Design Theory for Public e-Services.

Colesca, S.E., 2009. Understanding Trust in e-Government. *Inzinerine Ekonomika-Engineering Economics(3)*, (3), pp.7–15.

Council of Europe, 1950. *European Convention on Human Rights*, Rome.

Cukjati, D. & Todorovski, L., 2008. INTEGRATING E-SERVICES IN PUBLIC ADMINISTRATION: ANALYSIS OF EU RESEARCH PROJECTS AND INVOLVEMENT OF PARTICIPANTS FROM SEE REGION. In *Symposium proceedings of Second International Symposium on the Development of Public Administration in South East (SE) Europe*. pp. 19–20.

Dada, D., 2006. The Failure of E-Government in Developing Countries: A Literature Review. *The Electronic Journal on Information Systems in Developing Countries*, 26(1), pp.1–10.

Dais, A. et al., 2008. Introducing a Public Agency Networking Platform towards supporting Connected Governance. In *EGOV 2008*. Turin,Italy.

Dais, A., Nikolaidou, M. & Anagnostopoulos, D., 2009. Facilitating Business to Government Interaction Using a Citizen-Centric Web 2.0 Model. In C. Godart et al., eds. *Software Services for e-Business and e-Society SE - 12*. Springer Berlin Heidelberg, pp. 134–147.

Dais, A., Nikolaidou, M. & Anagnostopoulos, D., 2011. OpenSocialGov: A Web 2.0 Environment for Governmental E-Service Delivery. In *Electronic Government and the Information Systems Perspective, LNCS*. Springer Berlin Heidelberg.

Dara, S. & Fluhrer, S., 2014. FNR : Arbitrary length small domain block cipher proposal. *Cisco Systems, Inc.*

Davis, J., 2009. *Open Source SOA*, Manning Publications Co.

Dias, G.P., 2006. *Arquitectura de Suporte à Integração de Serviços no Governo Electrónico*. Universidade de Aveiro.

Dias, G.P., 2011. Q-Model: um modelo bidimensional de maturidade para o e-government. *RISTI: Iberian Journal on Information Systems & Technologies/Revista Ibérica de Sistemas e Tecnologias de Informação*, (7).

Dias, G.P., Gomes, H. & Zúquete, A., 2013. Privacy Policies in Web Sites of Portuguese Municipalities: An Empirical Study. In Á. Rocha et al., eds. *Advances in Information Systems and Technologies*. Springer Berlin Heidelberg, pp. 87–96.

Dias, G.P. & Narciso, T., 2010. Analysis of the potential for organizational interoperability improvement in local government. *Actas de la 5ª Conferência Ibérica de Sistemas y Tecnologias de Información*, I, pp.167–172.

Dias, G.P. & Rafael, J., 2007. A simple model and a distributed architecture for realizing one-stop e-government. *ECRA*, 6(1).

Dustdar, S. & Papazoglou, M.P., 2008. Services and Service Composition – An Introduction. *IT - Information Technology*, 2, pp.86–92.

Dutton, W. et al., 2005. The Cyber Trust Tension in E-government: Balancing Identity, Privacy, Security. *Information Polity*, 10(1/2), pp.13–23.

Ebrahim, Z. & Irani, Z., 2005. E-government adoption : architecture and barriers. *Business Process Management Journal*, 11(5), pp.589–611.

ENISA, 2009. *Privacy Features of European eID Card Specifications* I. Naumann, ed., ENISA.

Erl, T., 2005. *Service-Oriented Architecture: Concepts, Technology, and Design*, Prentice-Hall.

Erl, T. et al., 2009. *Web Service Contract Design and Versioning for SOA*, Prentice-Hall.

European Commission, 2010. Anex II to the Commission communication on interoperability - European Interoperability Framework (EIF).

European Commission, 2008. *Draft document as basis for EIF 2.0*,

European Commission, 2004. *European Interoperability Framework for Pan-European eGovernment Services (EIF), Version 1.0*, European Commision.

European Commission, 2003a. *Linking up Europe: the Importance of Interoperability for eGovernment Services*, IDA Program.

European Commission, 2003b. *The Role of eGovernment for Europe's Future*, Brussels.

Eynon, R., 2007. Breaking Barriers to eGovernment: Solutions for eGovernment, Deliverable 3. *eGovernment Unit, DG Information Society and Media, European Commission*, (29172).

Fallside, D.C. & Walmsley, P. eds., 2004. *XML Schema Part 0: Primer Second Edition*, W3C.

Feldkamp, D. et al., 2010. E-Government for Distributed Autonomous Administrations.

Fischer-Hübner, S. & Hedbom, H. eds., 2008. *PRIME Framework V3*, PRIME - Privacy and Identity Management for Europe.

Fountain, J.E., 2001. *Building the Virtual State. Information Technology and Institutional Change*, Washington DC: Bookings Institution Press.

Frois, C., 2007. Knowing Me , Knowing You : a vigilância enquanto objecto de estudo etnográfico. *Vide Science Technique Et Applications*, pp.1–10.

Gardini, S., Mattei, M.M. & Orelli, R.L., 2012. Gov 2 . 0 theory and practice for service delivery. , 62(1971), pp.122–127.

Germanakos, P., Christodoulou, E. & Samaras, G., 2007. A European Perspective of E-Government Presence - Where Do We Stand? The EU-10 Case. In *Electronic Government*. Springer, pp. 436–447.

Glazer, I. & Blakley, B., 2009. Identity and Privacy Strategies: In depth Research Overview. *Bourton Group*.

Gomes, H., Zúquete, A. & Dias, G.P., 2012. CITIZEN-SIDE HANDLING OF LIFE EVENT SERVICES. *WEBIST 2012 - 8th International Conference on Web Information Systems and Technologies*, pp.565–570.

Gomes, H., Zúquete, A. & Dias, G.P., 2011. PROCESSO DE AGREGAÇÃO DE ATRIBUTOS DE UM UTENTE COM GARANTIA DE PRIVACIDADE. *Patente PT-105979*.

Gottschalk, P., 2009. Maturity levels for interoperability in digital government. *Government Information Quarterly*, 26(1), pp.75–81.

Group, I.S., 2013. Midata: Towards a Personal Information Revolution. In *Digital Enlightenment Yearbook 2013*. IOS Press, pp. 202–224.

Gugliotta, A. et al., 2005. A Semantic Web Service-based Architecture for the Interoperability of E-government Services. In *Proceeding of the International Workshop on Web Information Systems Modeling*. Sidney, Australia.

Haas, H. & Brown, A. eds., 2004. *Web Services Glossary: W3C Working Group Note 11 February 2004*, World Wide Web Consortium (W3C).

Hagel III, J. & Rayport, J.F., 1997. The Comming Battle for Customer Information. *Harvard Business Review*, (January- February Reprint Number), pp.5–11.

Hashimoto, R., Ueno, N. & Shimomura, M., 2009. A design of usable and secure access-control APIs for mashup applications. In *Proceedings of the 5th ACM workshop on Digital identity management*. ACM, pp. 31–34.

Heikkinen, K. et al., 2004. Personalized View of Personal Information. *WSEAS Transactions on Information Science and Applications*, 2(4).

Hellman, R., 2010. Organisational barriers to interoperability. In P. Cunningham & M. Cunningham, eds. *eChallenges e-2010 Conference Proceedings*. IIMC International Information Management Corporation.

Hollingsworth, D., 1995. *Workflow Management Coalition The Workflow Reference Model*, Workflow Management Coalition.

Howard, C., 2014. Rethinking Post-NPM Governance: The Bureaucratic Struggle to Implement One-Stop-Shopping for Government Services in Alberta. *Public Organization Review*, pp.1–18.

Jaeger, P.T. & Thompson, K.M., 2003. E-government around the world : Lessons , challenges , and future directions. *+ Government Information Quarterly*, 20, pp.389–394.

Jeff, B., 2000. At the dawn of e-government: the citizen as customer. *Government Finance Review*, 16(5), p.15.

Jones, W., 2007. Personal Information Management. *Annual Review of Information Science and Technology*, 41(1), pp.453–504.

Jonsson, J. & Kaliski, B., 2003. Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1. *RFC3447*.

Josefsson, S., 2006. The Base16, Base32, and Base64 Data Encodings. *RFC4648*.

Kemp, R. & Moore, A.D., 2007. Privacy. *Library Hi Tech*.

Kirkham, T. et al., 2013. The Personal Data Store Approach to Personal Data Security. *Security & Privacy, IEEE*, 11(5), pp.12–19.

Kleek, M. Van & Hara, K.O., 2014. The Future of Social is Personal : The Potential of the Personal Data Store. In *Smart Societies*. Springer-Verlag.

Klischewski, R., 2004. Information integration or process integration? How to achieve interoperability in administration. In *Electronic Government: Proceedings of Third International Conference, EGOV 2004*. Zaragoza, Spain: Springer, pp. 57–65.

Kramer, A.D.I., Guillory, J.E. & Hancock, J.T., 2014. Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences*, 111(24), pp.8788–8790.

Kubicek, H. & Cimander, R., 2009. Three dimensions of organizational interoperability: Insights from recent studies for improving interoperability frameworks. *European Journal of ePractice*, (January), pp.1–12.

Kubicek, H. & Hagen, M., 2000. One-Stop-Government in Europe: An overview. In *One-Stop Government in Europe: Results from 11 National Surveys*. Bremen: University of Bremen, pp. 1–38.

Kuneva, M., 2009. Keynote Speech: Roundtable on Online Data Collection, Targetting and Profiling.

Lam, W., 2005. Barriers to e-government integration. *Journal of Enterprise Information Management*, 18(5), pp.511–530.

Lau, E., 2003. Challenges for E-Government Development. In *5th Global Forum on Reinventing Government*. Mexico City.

Leben, A. & Bohane, M., 2004. Architecture of an Active Life-Event Portal: A Knowledge-Based Approach. In *LNCS 3035*. pp. 147–156.

Li, C. et al., 2011. MRD : A Mashup Resource Discovery Approach Applying Semantics Indexing. In *IEEE ICC 2011 proceedings*. IEEE.

Lindgren, I. & Jansson, G., 2013. Electronic services in the public sector : A conceptual framework Electronic. *Government Information Quarterly*, 30(2), pp.163–172.

Lips, M., 2010. Rethinking citizen--government relationships in the age of digital identity: Insights from research. *Information Polity*, 15(4), pp.273–289.

Lips, M., Taylor, J. & Organ, J., 2010. Identity management in e-Government service provision. *Understanding E-Government in Europe: Issues and Challenges*, p.151.

Löfstedt, U., 2005. E-government - assessment of current research and some proposals for future directions. *International journal of public information systems*, 1(1), pp.39–52.

Lopes, R. & Shin, D., 2007. Controlled Sharing of Identity Attributes for Better Privacy. In *International Conference on Collaborative Computing: Networking, Applications and Worksharing, 2007. CollaborateCom 2007.* New York: IEEE Xplore Digital Library.

Marconi, A. & Pistore, M., 2009. Synthesis and Composition of Web Services. In M. Bernardo, L. Padovani, & G. Zavattaro, eds. *Formal Methods for Web Services SE - 3*. Springer Berlin Heidelberg, pp. 89–157.

Martin, D. et al., 2007. Bringing Semantics to Web Services with OWL-S. In *World Wid Web*. Springer US, pp. 243–277.

Masrom, M., Lim, E.A. & Din, S., 2013. Security and Quality Issues in Trusting E-Government Service Delivery. *Managing Trust in Cyberspace*, p.197.

Mccallister, E., Grance, T. & Scarfone, K., 2010. Guide to Protecting the Confidentiality of Personally Identifiable Information (PII): Recommendations of the National Institute of Standards and Technology. *Nist Special Publication 800-122*.

Merrill, D., 2009. Mashups: The new breed of Web app. *IBM DeveloperWorks*.

Microsoft, 2006. The Identity Metasystem : Towards a Privacy-Compliant Solution to the Challenges of Digital Identity. *Card Technology*, (October).

Mitra, N. & Lafon, Y. eds., 2007. *SOAP Version 1.2 Part 0: Primer (Second Edition)*, W3C.

Modinis-IDM, 2005. Common Terminological Framework for Interoperable Electronic Identity Management.

Momotko, M. et al., 2007. An Architecture of Active Life Event Portals: Generic Workflow Approach. In *LNCS 4656*. Springer.

Momotko, M. et al., 2006. Towards Implementation of Life Events Using Generic Workflows. In *eGOV06*. Brunel University, London.

Mydex, 2010. The Case for Personal Information Empowerment: The rise of the personal data store. *World*, pp.1–44.

Nadalin, A. et al. eds., 2009. *WS-SecurityPolicy 1.3*, OASIS.

Narayanan, A. et al., 2012. A Critical Look at Decentralized Personal Data Architectures.

Ndou, V., 2004. E-government for developing countries: opportunities and challenges. *The Electronic Journal of Information Systems in Developing Countries*, 18.

Nissenbaum, H., 2004. Privacy as contextual integrity. *Washington Law Review*, pp.101–139.

Nordfors, L. et al., 2009. *eGovernment of Tomorrow - Future Scenarios for 2020*, VINNOVA.

Novakouski, M. & Lewis, G.A., 2012. Interoperability in the e-Government Context. *TECHNICAL NOTE CMU/SEI-2011-TN-014*.

OASIS, 2007. *Web Services Business Process Execution Language Version 2.0*, OA.

OECD, 2013. OECD GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA. , pp.11–37.

Overeem, A. Van, Witters, J. & Peristeras, V., 2007. An Interoperability Framework for Pan-European E-Government Services (PEGS). In *Proceedings of the 40th Hawaii International Conference on System Sciences*. IEEE, pp. 1–10.

Palvia, S.C.J. & Sharma, S.S., 2007. E-government and e-governance: definitions/domain framework and status around the world. In A. Agarwall & V. V. Ramana, eds. *Foundations of E-government. ICEG 5th International Conference on E-governance*. Hyderabad, India.

Pappa, D. & Makropoulos, C., 2004. Designing a Brokerage Platform for the Delivery of E-government Services to the Public. In *LNCS 3035*. Springer.

Pfister, J. & Schwabe, G., 2013. The Landscape of Electronic Data Safes and their Adoption in E-Government and E-Business. In *46th Hawaii International Conference on System Sciences*. IEEE Computer Society, pp. 1963–1972.

Pfitzmann, A. & Hansen, M., 2009. A terminology for talking about privacy by data minimization : Pseudonymity , and Identity Management. *http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.32.pdf*, pp.1–86.

Prime, 2004. Me , Myself and I! Manage your identities safely. *Prime*.

Projecto Cartão de Cidadão, 2006. *Relatório Final da Prova de Conceito - Projecto Pegasus*,

Raab, C.D., 2005. Perspectives on "personal identity". *BT Technology Journal*, 23(4), pp.15–24.

Ragouzis, N. et al. eds., 2008. *Security Assertion Markup Language (SAML) V2. 0 Technical Overview* Comitee Dr., OASIS.

Reed, D., Johnston, J. & David, S., 2011. *The Personal Network: A New Trust Model and Business Model for Personal Data*, Connect.Me.

Relyea, H.C., 2002. E-gov: Introduction and overview. *Government information quarterly*, 19(1), pp.9–35.

Roosendaal, A. et al. eds., 2009. Analysis of Privacy and Identity Management throughout Life. *PrimeLife: Privacy and Identity Management in Europe for Life*.

Roundtree, D., 2008. *Federated Identity Primer*, Syngress.

Sanati, F. & Lu, J., 2009. Multilevel Life-Event Abstraction Framework for e- Government Service Integration. In *Academic Conferences International (ACI)*. pp. 550–558.

Schedler, K. & Proeller, I., 2000. *New Public Management.*, UTB.

Scholl, H.J. & Klischewski, R., 2007. E-government integration and interoperability: framing the research agenda. *International Journal of Public Administration*, 30(8-9), pp.889–920.

Sheng, Q.Z. et al., 2014. Web services composition: A decade's overview. *Information Sciences*, 280, pp.218–238.

Shroff, M. & Fordham, A., 2010. " Do you know who I am?" Exploring identity and privacy. *Information Polity*, 15(4), pp.299–307.

Siebeck, R.G. & Wolfgang, W., 2009. Cloud-based Enterprise Mashup Integration Services for B2B Scenarios Categories and Subject Descriptors. In *Proceeding of the 2nd workshop on Mashup and Enterprise Mashups (in conjunction with WWW2009), MEM2009*. Madrid, Spain.

Silcock, R., 2001. What is e-government. *Parliamentary affairs*, 54(1), pp.88–101.

Silva, E.M.G. da, 2011. *User-centric Service Composition - Towards Personalised Service Composition and Delivery*. University of Twente, The Netherlands.

Smith, R.E., 2001. *Authenticaton: From Passwords to Public Keys*, Addison-Wesley Professional.

Soares, D. & Amaral, L., 2011. Information Systems Interoperability in Public Administration : Identifying the Major Acting Forces through a Delphi Study. *Electronic Commerce Research*, 6(1).

Solove, D.J., 2006. A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3), pp.477–564 ST – A taxonomy of privacy.

Solove, D.J., 2007. I've Got Nothing to Hide and Other Misunderstandings of Privacy. *San Diego L. Rev.*, 44(May), p.745.

Soriano, J. et al., 2008. Enhancing User-Service Interaction Through a Global User-Centric Approach to SOA. In *Fourth International Conference on Networking and Services*. IEEE Computer Society, pp. 194–203.

Sroga, M., 2008. Access-eGov - Personal Assistant of Public Services. In *Computer Science and Information Technology, 2008. IMCSIT 2008. International Multiconference on*. IEEE, pp. 421–427.

Tambouris, E. et al., 2008. The role of interoperability in eGovernment applications: An investigation of obstacles and implementation decisions. In *ICDIM 2008*. London: IEEE.

Todorovski, L. et al., 2006. Methodology for Building Models of Life Events for Active Portals. In *EGOV 2006*. Cracow, Poland.

Todorovski, L., Kunstelj, M. & Vintar, M., 2007. Reference Models for e-Services Integration based on Life-Events. In *LNCS 4656*. Springer.

Trochidis, I., Tambouris, E. & Tarabanis, K., 2007. An Ontology for Modeling Life-Events. In *IEEE International Conference on Services Computing (SCC 2007)*. pp. 719–720.

Trochidis, I., Tambouris, E. & Tarabanis, K., 2006. Identifying common workflow patterns in life-events and business episodes. In *The second International Conference on e-Government*. pp. 234–243.

Trochidis, I., Tambouris, E. & Tarabanis, K., 2008. One Stop Government: A Literature Review. In *6th Eastern European eGov Days*. Prague.

UMIC, 2011. Plataforma de Interoperabilidade. Available at: http://www.umic.pt/index.php?option=com_content&task=view&id=2687&Itemid=112 [Accessed May 17, 2012].

United Nations, 2008. *E-Government Survey 2008 - From e-Government to Connected Governance*, New York: United Nations.

United Nations, 2010. *E-Government Survey 2010 - Leveraging e-government at a time of financial and economic crisis*, New York: United Nations.

United Nations, 2012. *E-Government Survey 2012 - E-Government for the People*, New York: United Nations.

United Nations, 2014. *E-Government Survey 2014 - E-Government for the Future We Want*, New York: United Nations.

United Nations & American Society for Public Administration, 2002. *Benchmarking E-government: A Global Perspective*, New York: U. N. Publications.

United Nations General Assembly, 1948. *The Universal Declaration of Human Rights, General Assembly resolution 217 A (III)*, http://www.un.org/en/documents/udhr/index.shtml.

Vaz, A., 2007. Segurança da Informação, Proteção da Privacidade e dos Dados Pessoais. *Nação e Defesa*, 117(3), pp.35–63.

Vedamuthu, A.S. et al. eds., 2007. *Web Services Policy 1 . 5 - Primer*, W3C.

Vintar, M., Kunstelj, M. & Leben, A., 2002. Delivering Better Quality Public Services Through Life-Event Portals. In *10th NISPAcce Annual Conference*. Cracow, Poland.

Vrieze, P. De et al., 2009. Process-oriented Enterprise Mashups. In *2009 Workshops at the Grid and Pervasive Computing*.

Warner, J. & Chun, S.A., 2008. A citizen privacy protection model for e-government mashup services. In *Proceedings of the 2008 international conference on Digital government research*. Digital Government Society of North America, pp. 188–196.

Westin, A.F., 1967. *Privacy and freedom*, New York, NY: Athenäum.

Westin, A.F., 2003. Social and Political Dimensions of Privacy. *Journal of Social Issues*, 59(2), pp.1–37.

Whitley, E.A., 2009. Informational Privacy, Consent and the Control of Personal Data. *Social Research*, pp.1–13.

Wimmer, M.A. & Tambouris, E., 2002. Online One-Stop Government: A working framework and requirements. In *Proceedings of the IFIP World Computer Congress*. Montreal: Springer.

Windley, P., 2005. *Digital identity*, O'Reilly Media, Inc.

World Economic Forum, 2011. *Personal Data: The Emergence of a New Asset Class*, World Economic Forum.

Xie, L., Xu, L. & Vrieze, P. De, 2010. Process Modelling in Process-oriented Enterprise Mashups. In *2010 the 2nd IEEE International Conference on Information Management and Engineering, IEEE ICIME 2010*. Chengdu, China.

Yildiz, M., 2007. E-government research: Reviewing the literature, limitations, and ways forward. *Government Information Quarterly*, 24(3), pp.646–665.

Zarandioon, S., Yao, D. & Ganapathy, V., 2009. Privacy-aware Identity Management for Client-side Mashup Applications ∗. *University Computing*, pp.21–30.

Zúquete, A., Gomes, H. & Teixeira, C., 2014. Personal Identification in the Web Using Electronic Identity Cards and a Personal Identity Provider. In D. Naccache & D.

Sauveron, eds. *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, pp. 160–169.