A importância das Infra-estruturas de Chave Pública no Comércio Electrónico de Conteúdos Digitais

Carlos Serrão

Instituto Superior de Ciências do Trabalho e da Empresa

Setembro de 2002

Orientador Científico: Professor Doutor Cordeiro Gomes

A Nova Economia, baseada essencialmente na Internet, depende em muito da validade e segurança da informação. O comércio em geral não poderia existir se laços de confiança entre vendedor e comprador não fossem estabelecidos. No Comércio Electrónico este aspecto é de especial importância devido à inexistência do tradicional contacto físico entre ambos.

Os novos modelos de comercialização de conteúdos digitais através de meios electrónicos levantam igualmente desafios de segurança e de gestão e protecção da propriedade intelectual que devem ser encarados de uma forma séria utilizando um conjunto de medidas de segurança eficientes.

A confiança é igualmente importante para este tipo de Comércio Electrónico. Apesar do problema de confiança não depender somente de uma componente tecnológica, não há dúvida de que esta representa igualmente um papel importante, que passa pela utilização de tecnologia criptográfica, para garantir princípios fundamentais: privacidade, autenticação, integridade e não-repúdio. O modelo de confiança ubíquo que lhe está subjacente designa-se por PKI ou Infra-estrutura de Chave Pública e é o alvo da atenção da presente dissertação de Mestrado, em conjunto com o estudo da sua aplicabilidade na gestão e protecção da propriedade intelectual e no Comércio Electrónico de conteúdos digitais.

A importância das Infra-estruturas de Chave Pública no Comércio Electrónico de Conteúdos Digitais

Carlos Serrão

DISSERTAÇÃO DE MESTRADO EM GESTÃO DE SISTEMAS DE INFORMAÇÃO

Apresentada ao Instituto Superior de Ciências do Trabalho e da Empresa para obtenção do grau de Mestre em Gestão de Sistemas de Informação.

Setembro de 2002

Professor Doutor	Orientador Científico da dissertação de Mestrado
Cordeiro Gomes	Professor Convidado do ISCTE

INSTITUTO SUPERIOR DE CIÊNCIAS DO

TRABALHO E DA EMPRESA

Dedicatória

Gostaria de agradecer e dedicar este meu trabalho a uma série de pessoas que sempre me apoiaram e que me têm transmitido toda a força necessária para conseguir concluir com sucesso esta minha missão.

O meu primeiro agradecimento e dedicatória vão para o meu primeiro orientador da dissertação de Mestrado, o Eng. José Guimarães, ao qual uma partida do destino ceifou a vida impedindo-o de ver concluído este meu trabalho que era igualmente o seu. De qualquer forma é minha convicção de que onde quer que ele esteja, acompanha o trabalho da sua anterior equipa. Foi dele que partiu a ideia para o tema desta dissertação, o qual abracei de imediato e resolvi dedicar todo o meu esforço, que agora concluo.

Uma dedicatória muito especial vai de igual forma para a minha esposa, Fátima, e para o meu filhote David. Obrigado por todo o vosso amor, compreensão e ajuda. Agora terei mais tempo para vocês. Amo-vos muito.

Dedico-a igualmente aos meus pais, que me proporcionaram todas as condições necessárias para que pudesse evoluir na minha educação e realizasse este meu Mestrado. Um beijinho muito especial à minha mãe por todo o seu apoio e motivação.

Gostaria de expressar de igual forma os meus agradecimentos ao Joaquim, ao Daniel e ao João pela sua ajuda na revisão ortográfica.

Por último, parte do mérito da conclusão deste trabalho vai para o meu actual coordenador, Professor Doutor Cordeiro Gomes, por ter aceite substituir e continuar a coordenação do meu anterior orientador, e por ter dado todo o seu apoio a este trabalho. Obrigado por toda a sua ajuda nos mais variados aspectos e em especial pela sua dedicação e orientação.

A todos os outros cujo nome não foi aqui mencionado, o meus mais sinceros agradecimentos.

Índice Geral

Índice de Imagens

Índice de Tabelas

1 INTRODUÇÃO

O mercado dos conteúdos digitais encontra-se em grande evolução [SGDD00]. Sendo um mercado demasiadamente complexo, os conteúdos digitais levantam inúmeros problemas, grande parte deles relacionados com a gestão da propriedade intelectual. Este foi um dos principais motivos que levou o autor à escolha do tema para a elaboração desta dissertação. Outro dos motivos que se prende com esta escolha está relacionado com a participação recente em projectos de Investigação e Desenvolvimento patrocinados pela Comissão Europeia (OKAPI[1], OCTALIS[2], OCCAMM[3]) que estão directamente ligados com a protecção e gestão dos direitos de autor de conteúdos digitais. Ao longo desta participação, foi possível constatar que a solução ideal para estes problemas ainda está longe de ser encontrada e também que a maior parte das soluções existentes para lidar com os problemas associados à gestão da propriedade intelectual de conteúdos digitais em ambientes abertos são, na sua maioria, proprietárias.

A presente dissertação visa demonstrar através de uma aplicação prática que é possível desenvolver e implementar sistemas capazes de difundir conteúdos digitais de forma segura, salvaguardando os direitos de autor. Pretende-se igualmente indicar alguns caminhos que possam contribuir para melhorar alguns aspectos desta problemática, propondo uma aproximação baseada na combinação de Infra-estruturas de Chave Pública (PKI) em conjunto com uma solução de gestão de direitos digitais, que possa ser utilizada no Comércio Electrónico de Conteúdos Digitais.

Aspectos como a Privacidade, Autenticação, Integridade e Não-Repúdio são importantes para a implementação e realização deste tipo de Comércio Electrónico e como tal foram incorporados. Particular atenção foi dada à aplicação das PKI à protecção dos direitos de autor na comercialização electrónica de conteúdos digitais, sendo este o alvo principal do estudo da presente dissertação de Mestrado.

A aplicação prática demonstrou, numa situação de testes, ser possível a utilização do sistema por utilizadores reais na aquisição de música digital através de meios electrónicos. Na realização desta aplicação foram considerados o trabalho desenvolvido pela iniciativa OPIMA e a sua implementação pelo projecto Europeu OCCAMM, partindo-se assim para a adaptação dos componentes desenvolvidos e para a incorporação da gestão dos direitos de autor na PKI.

Este trabalho aponta claramente um caminho que segue na direcção da implementação de uma solução para a gestão da propriedade intelectual com uma forte ligação às PKI. Assim, esta dissertação sugere a

[1] OKAPI – Open Kernel for Access to Protected Interoperable interactive services (ACTS AC051)

[2] OCTALIS - Offer of Contents through Trusted Access LInkS (ACTS AC242)

[3] OCCAMM - Open Components for Controlled Access to Multimedia Material (IST IST-2000-11443)

criação de uma PKI para suportar todos os aspectos de segurança essenciais à protecção da integridade do conteúdo digital, assim como, das diversas entidades intervenientes no processo de comercialização electrónica do mesmo. Outro dos caminhos sugeridos foca a utilização do XML não apenas como a tecnologia que define o protocolo de comunicação entre estes intervenientes como se apresenta como um substituto para formatos de credenciais em PKI tradicionais.

A evolução das comunicações, e em particular o desenvolvimento da Internet, cria as condições para que o mercado do futuro seja cada vez mais global e electrónico [ECRTBD00], representando uma mudança profunda na forma de conduzir negócios. Esta mudança tem vindo a ser amplamente reconhecida por analistas e empresários, não existindo, todavia, certezas sobre quando e como se irá fazer sentir de forma maciça o seu impacto. No entanto, o processo de transformação já está em marcha, atingindo proporções significativas nos Estados Unidos e na Europa [EBMOC99, CENI99].

A visão prevalecente é a de que a Economia organizar-se-á em torno de vastos sistemas de negócio electrónico constituídos por redes de fornecedores, distribuidores e clientes, que utilizarão meios electrónicos como plataformas base para colaborarem e competirem no mercado [CENI99].

A criação desta nova forma de organização, frequentemente designada por Nova Economia, reside na possibilidade de as empresas e organizações em geral se reinventarem, aproveitando o seu conhecimento e as suas potencialidades internas para, com base nas possibilidades oferecidas pela tecnologia, alterarem cadeias de valor, redefinirem os seus processos de negócio, aumentarem a produtividade e globalizarem-se [CENI99].

Esta Nova Economia, baseada essencialmente na Internet, depende em muito da validade e da segurança da informação [PKISEC01]. O comércio não poderá existir se a confiança entre vendedor e comprador *on-line* não for estabelecida.

A confiança sempre representou um papel fundamental nos negócios. Como percursor fundamental do comércio, a confiança está incorporada em todas as estruturas e processos de mercado. No entanto, o Comércio Electrónico alterou profundamente essas estruturas e processos, e o próprio conceito de confiança sofreu igualmente modificações [ECRTBD00].

Para que estes laços se fortaleçam e se tornem mais eficazes, três componentes da segurança de informação têm vindo a marcar o panorama: a criptografia, os certificados digitais, e as PKI [ECRTBD00, PKISEC01]. Estes componentes encontram-se interligados entre si, ajudando as organizações a construírem e a reformularem os seus negócios para a *World Wide Web*, enquanto asseguram que a informação vital dos consumidores e da própria organização seja mantida confidencial. Os certificados digitais são importantes para os diferentes tipos de negócio, ajudando os consumidores e os negócios a verificar a fonte da informação, determinando/garantindo a autenticidade de entidades, aplicações de *software* e outros produtos [IGSAV99].

A maturação deste tipo de tecnologias ao longo dos últimos tempos tem ajudado em muito o crescimento da referida Nova Economia. Para além disso, estas tecnologias têm permitido o comércio baseado na Internet e a utilização da Web pelos negócios, o que sem a utilização da criptografia, dos certificados digitais e das PKI seria de todo impensável [BEC01, ECRTBD00].

Num estudo recente realizado pela *CommerceNet* foram identificadas as principais barreiras e inibidores do Comércio Electrónico. De acordo com este estudo as mais importantes barreiras ao crescimento do Comércio Electrónico continuam a estar relacionadas com as áreas de segurança: Segurança e Encriptação, Confiança e Risco, Autenticação dos Utilizadores e inexistência de Infra-estruturas de chave pública são os aspectos mais citados neste estudo [BEC01, IGSAV99].

Prevê-se que a comercialização de conteúdos digitais seja uma das áreas do Comércio Electrónico a sofrer um impulso bastante grande [STDMB02]. Outras áreas que beneficiarão igualmente desse impulso são, por exemplo: iTV[4], TdT[5], MoD[6], VoD[7], Música digital, *e-Learning*, entre tantas outras.

As tecnologias digitais são excelentes ferramentas que permitem tornar os conteúdos, tanto em termos de facilidade como de custos de criação, melhores do que os obtidos por via das suas congéneres analógicas. De igual forma, os conteúdos digitais oferecem regra geral mais funcionalidades e de qualidade superior. Empresas e consumidores ganham em tempo, espaço e qualidade do acesso, ao mesmo tempo que todo o processo de gestão se simplifica e torna mais flexível [TVOC00]. Para as empresas de fornecimento de serviços, os conteúdos digitais oferecem funcionalidades que não poderiam ter sido conceptualizadas outrora [IPMF00, TNYMBK00].

Este tipo de tecnologias abriu, assim, as portas para novas possibilidades no mundo da publicação electrónica. Imagine-se um mundo em que o conteúdo flúi de dispositivo para dispositivo e de utilizador para utilizador de uma forma transparente [TEPTP02]. A possibilidade dos conteúdos se adaptarem às necessidades dos consumidores tornou-se uma realidade. Os pagamentos podem ser realizados de forma transparente e em tempo real sem que a utilização seja afectada por isso [TEPTP02].

Criadores e/ou distribuidores podem ainda criar diferentes versões do mesmo conteúdo, procurando assim diversificar as fontes de rendimento. Este poderia ser dividido em partes mais pequenas, de forma a poderem receber micro-pagamentos por partes do conteúdo e macro-pagamentos pela totalidade do mesmo. Por exemplo, no caso da música poder-se-á receber micro-pagamentos por cada faixa musical e macro-pagamentos pela totalidade do álbum [TEPTP02, UDRMS01].

Todavia, o valor intrínseco dos conteúdos digitais é actualmente entendido pelos utilizadores como sendo volúvel. Um dos exemplos mais concretos desta afirmação é aquilo que se designa por "fenómeno" MP3 [MPEGA00].

É perfeitamente aceitável que aqueles que detêm os direitos de autor sobre as músicas se sintam relutantes em aderir a esta mudança, já que para eles a tecnologia MP3 não é percepcionada como uma alternativa facilitadora da melhoria da sua experiência individual de divulgação da música mas sim como um meio de espoliar os detentores dos direitos dos benefícios que lhes serão devidos [TVOC00].

[4] iTV – Televisão Interactiva

[5] TdT – Televisão Digital Terrestre

[6] MoD – *Music on Demand*

[7] VoD – *Video on Demand*

O caso do MP3 é apenas um exemplo de como a gestão e protecção dos direitos de propriedade intelectual se tornou um aspecto crucial nos dias que correm como factor capaz de influenciar o desenvolvimento do Comércio Electrónico envolvendo conteúdos digitais [TVOC00].

Conhecem-se casos em que a segurança não foi eficaz apesar de terem sido aplicadas medidas de protecção de direitos de autor. É o caso do sistema de encriptação CSS – *Content Scrambling System*, utilizado pelos DVD comerciais, que foi quebrado em pouco tempo [CCSS99], permitindo a cópia e a reprodução ilegal [CCSS99].

O Comércio Electrónico de conteúdos digitais gera enormes desafios de resolução complexa, cuja solução reside no controlo do acesso e utilização dos mesmos [STDMB02, TVOC00]. Num mundo digital a gestão deste controlo de acesso e utilização e dos correspondentes direitos é facilitada pela utilização de soluções DRM – *Digital Rights Management*.

Estas soluções surgiram para proteger e gerir o comércio, a detenção da propriedade intelectual, e os direitos de confidencialidade dos produtores e detentores do conteúdo digital sempre que este flúi pela cadeia de valor, do criador para o distribuidor e para o consumidor ou do consumidor para outros consumidores [UDRMS01]. Protege e controla o conteúdo de uma forma persistente através de regras definidas pelo autor deste e dos direitos detidos pelo utilizador. As soluções DRM podem ser utilizadas para controlar e acompanhar os acessos autorizados, usando essa informação mais tarde para efeitos financeiros ou de Marketing [UDRMS01].

A confiança e o controlo são dois aspectos nucleares relacionados com as DRM. Estas soluções lidam com a encriptação do conteúdo e informação, estando integradas na organização ao nível da infra-estrutura. As organizações utilizam-nas para gerirem os dados encriptados, as chaves e a informação dos utilizadores [UDRMS01].

Actualmente, as soluções DRM ainda não se assumiram como amplamente aceitáveis para todos os actores deste grande palco do Comércio Electrónico de conteúdos digitais, uma vez que ainda existem problemas associados com a utilização dos mesmos [DRBSA02].

Uma potencial solução para estes problemas consiste na convergência tecnológica entre as soluções de DRM e as PKI [TVOC00, STDMB02]. De acordo com um estudo realizado pela União Europeia [DRBSA02], devem ser encontradas sinergias entre estas, sendo reconhecido o potencial de evolução das PKI que permitirá a incorporação futura de funcionalidades de gestão de direitos digitais (DRM). Esta nova solução deverá ir de encontro às diferentes necessidades, diferentes modelos económicos e soluções técnicas [ECRTBD00]. A convergência entre as soluções DRM e as PKI tem estado e está representada em algumas actividades de normalização (OPIMA (ver Capítulo 4), MPEG-4, MPEG-21) no que diz respeito à especificação de identificadores digitais de dados e a interoperabilidade dos diversos métodos de gestão de conteúdos multimédia [DRBSA02].

Como referido, a presente dissertação propõe uma solução mista DRM/PKI para o Comércio Electrónico de conteúdos digitais em segurança, tendo por base de implementação o trabalho realizado no âmbito de um projecto Europeu (OCCAMM), no qual o autor participou activamente.

Pela importância que as Infra-estruturas de Chave Pública têm no desenvolvimento do Comércio Electrónico, o Capítulo 2 apresenta de uma forma exaustiva um estudo sobre as PKI, apresentando-se igualmente algumas das tendências a considerar no desenvolvimento das mesmas.

No Capítulo 3, apresenta-se uma solução DRM desenvolvida no âmbito de um grupo de normalização designado por OPIMA e a sua implementação realizada por um projecto de Investigação e Desenvolvimento Europeu (OCCAMM).

No Capítulo 4, como já foi referido, é apresentada uma solução mista DRM/PKI, desenvolvida no âmbito desta dissertação, e implementada (código apresentado no Anexo H) com base na iniciativa OPIMA e no trabalho desenvolvido no projecto OCCAMM.

No Capítulo 5, são apresentados os testes de utilização real que foram efectuados com a solução desenvolvida. São igualmente apresentados os resultados destes e apontados alguns dos aspectos a melhorar no sistema.

Por último (Capítulo 6), são expostas as conclusões do trabalho desenvolvido sendo igualmente indicadas algumas direcções para desenvolvimentos futuros.

2 AS INFRA-ESTRUTURAS DE CHAVE PÚBLICA

2.1 Introdução

Este capítulo tem como objectivo principal introduzir o tema das PKI fazendo um levantamento e uma análise das mesmas. Pretende dar o enquadramento teórico necessário em torno das PKI para o trabalho que será apresentado nos capítulos seguintes (em particular no Capítulo 4 e Capítulo 5).

No mundo dos nossos dias, em que as Tecnologias de Informação reinam e impõem a sua lógica, tornam-se cada vez mais importantes e significativos aspectos como a Segurança da Informação [BEC01]. Quando a tecnologia Internet, em particular a *World Wide Web*, se tornou apetecível para exploração comercial, maior interesse foi sendo suscitado, e cada vez mais aplicações empresariais foram sendo desenvolvidas tendo como base a tecnologia *Web*. No entanto, toda esta globalização dos negócios tornou-os igualmente mais vulneráveis a diferentes tipos de ameaças para os quais não estavam totalmente preparados [TRASOTI00, CEICOM97].

As Infra-estruturas de Chave Pública (PKI) fazem, cada vez mais, parte das arquitecturas de segurança das organizações [PKIEG01]. Estas proporcionam um ponto focal para muitos aspectos da gestão de segurança, funcionando igualmente como impulsionadoras da utilização de um crescente número de aplicações de segurança. Muitos dos protocolos utilizados na Internet (correio electrónico seguro, acesso *Web*, Redes Privadas Virtuais (VPN)) e dos sistemas de autenticação de utilizadores através de "*single sign-on*" (SSO) utilizam certificados de chave pública e como tal necessitam de soluções PKI para funcionarem correctamente [UPKICSDC99, PKIKSEC01].

As tecnologias PKI proporcionam importantes vantagens para as entidades que as utilizam, nomeadamente [UPKICSDC99]:

- Redução do número de eventos "*sign-on*" requeridos pelos utilizadores finais – ou o "*single sign-on*";
- Redução da utilização do suporte papel e melhoria da eficiência do fluxo de trabalho através de processos de negócio mais automáticos e seguros;
- Optimização da produtividade da força de trabalho;
- Reduzidos requisitos de treino para os utilizadores finais relacionados com os serviços de segurança.

A procura de tecnologia PKI tem, recentemente, atraído a atenção de muitos. Todos os dias nos *media* da especialidade se pode ler com frequência a promessa de serviços de autenticação e não-repúdio

proporcionado pela utilização de técnicas de assinatura, e sobre serviços de confidencialidade e gestão de chaves baseadas na combinação de criptografia simétrica e assimétrica, todas estas proporcionadas pela utilização de uma tecnologia de suporte designada por PKI [AVTRELRIS97, WSCRTS97].

Os fundamentos em que se baseiam as PKI são já conhecidos acerca de duas décadas com a invenção da criptografia de chave pública. No entanto, a tecnologia PKI apenas teve o seu desenvolvimento comercial nos últimos anos, com a crescente procura comercial de serviços PKI por parte das organizações [PKIIMES01, TRWMTRRI98].

A segurança electrónica depende de processos e serviços que permitam a construção de uma solução segura para a distribuição de informação de negócio e serviço através da rede. Estes processos e serviços deverão ser capazes de garantir:

- Identificação: processo de reconhecimento de um determinado indivíduo;
- Autenticação: processo através do qual se prova e verifica determinada informação;
- Autorização: processo de determinar o que uma entidade está autorizada a realizar;
- Integridade: processo de assegurar que a informação é inalterada;
- Confidencialidade ou Privacidade: processo de manutenção de informação secreta;
- Não Repúdio: processo que significa que não se pode negar a ter feito algo.

Todos estes serviços são utilizados de uma forma ou de outra no nosso dia a dia. O desafio consiste na reprodução de serviços semelhantes no mundo do Comércio e Negócio Electrónico. As técnicas que são utilizadas para criar os análogos electrónicos destes serviços são baseadas em criptografia [CATKEC00, TIMCP97].

As PKI proporcionam ferramentas que permitem a disponibilização de serviços de segurança baseados em criptografia. Outras infra-estruturas que utilizam apenas criptografia simétrica (ver secção 2.2.1) têm vindo a ser utilizadas de forma tentativa, mas com pouco sucesso devido a problemas associados com a sua gestão e escalabilidade [UPKINF99]. As PKI permitem a criação de identidades e a confiança a elas associada para processos de identificação e autenticação, e gerem a encriptação de chave pública/privada, que proporciona uma solução muito mais escalável que as suas anteriores congéneres [UPKICSDC99, AHVCERT00].

As PKI, tal como o próprio nome indica, pressupõe a existência de uma infra-estrutura. Tal como qualquer outra infra-estrutura, o seu funcionamento é melhor quando é totalmente transparente para os utilizadores e entidades que a utilizam. A utilização de chaves públicas/privadas e certificados para assinar correio electrónico, autenticar *sites* de *Web*, validar transacções e outras funções, têm boa aceitação porque "escondem" o mecanismo das PKI utilizado para desempenhar estas actividades [WSCRTS97].

Na área da tecnologia PKI, grandes avanços têm sido realizados nos últimos anos, no campo da normalização. Para além das recomendações do X.509 do *International Telecommunications Union* (ITU) e das normas PKCS (*Public-Key Cryptographic Standards*) do RSA *Laboratories*, o trabalho mais significativo

nesta área tem sido realizado pelo *Internet Engineering Task Force* (IETF) através do grupo de trabalho PKI X.509 (PKIX) [UPKICSDC99].

Uma área em que as PKI têm tido um sucesso bastante significativo ocorre com a utilização de certificados SSL[8] de servidor. Muitas aplicações dependem da privacidade e integridade derivada de uma sessão SSL estabelecida com um servidor de *Web* para processar transacções de Comércio Electrónico seguras [ECRTBD00]. A razão para o sucesso desta aplicação de certificados é que ela é totalmente (ou quase) transparente para o utilizador final, e todas as funcionalidades necessárias de suporte estão directamente embebidas nos *browsers* da *Web*. A utilização de aspectos mais avançados das PKI tal como a autenticação de clientes não está bem integrada o que resulta numa menor utilização do que os certificados de servidor [WSCRTS97].

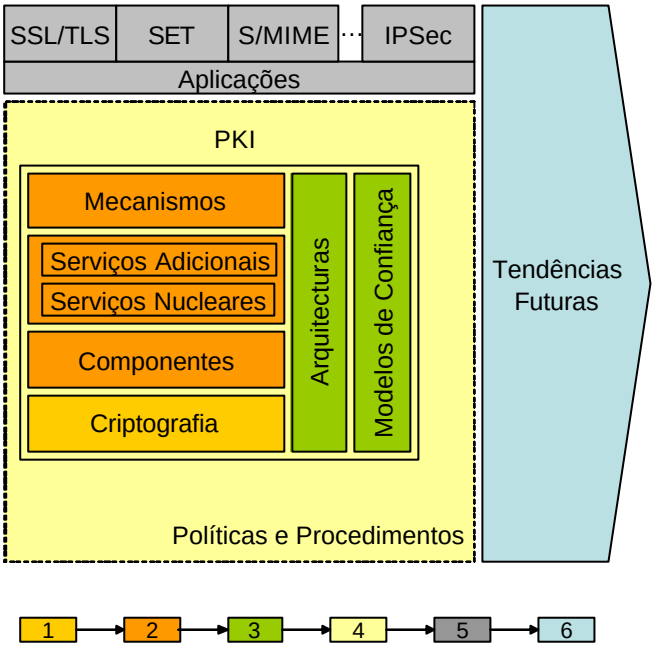


Figura 2.1 Estrutura e Organização do Capítulo

Na Figura 2.1 apresentam-se os principais elementos de uma solução PKI, aplicações existentes e tendências futuras:

Criptografia: nesta parte serão abordados os princípios base da criptografia e descritos alguns dos algoritmos mais relevantes;

Componentes, Serviços e Mecanismos: ao longo destas secções serão identificados e descritos os principais componentes das PKI, os principais serviços oferecidos pelas mesmas, assim como são apresentados alguns dos mecanismos base das PKI;

Arquitecturas e Modelos de Confiança: nestas secções são apresentadas as principais arquitecturas das PKI assim como os principais modelos de confiança que podem ser implementados recorrendo às mesmas;

[8] *Secure Sockets Layer*

Políticas e Procedimentos: ao longo desta secção serão descritos algumas das políticas e procedimentos necessários para a implementação e operação das PKI;

Aplicações: nesta secção são apresentadas algumas aplicações das PKI em soluções de segurança que se encontram a funcionar nos nossos dias;

Tendências Futuras: finalmente, nesta secção são apresentadas algumas das principais tendências que poderão influenciar as PKI do futuro.

Seguidamente, cada uma destas partes é abordada e apresentada com um maior grau de detalhe.

2.2 A Tecnologia Criptográfica

A criptografia consiste numa colecção de técnicas que permitem manter a informação segura. A utilização da criptografia permite a transformação de informação inteligível em informação ininteligível para que não possa ser perceptível para receptores não autorizados. A informação pode ser de novo transformada em informação inteligível para que o receptor autorizado possa ter acesso à mesma [NSEAS00, RSALFAQ00].

Os sistemas de criptografia moderna consistem essencialmente em dois processos complementares: a encriptação e desencriptação (Figura 2.2) [UPKICSDC99, PKIIMES01].

- Encriptação: o processo através do qual uma mensagem (original) é transformada numa outra mensagem (encriptada) utilizando uma função complexa e uma chave criptográfica;
- Desencriptação: o processo inverso do anterior, em que a informação encriptada é transformada de novo na informação original, utilizando uma função complexa e uma chave criptográfica.

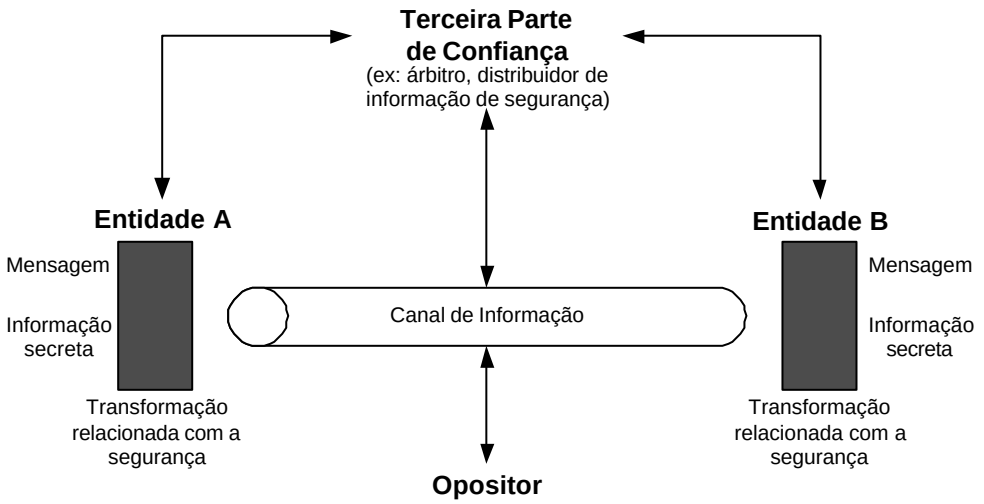


Figura 2.2 Modelo de Segurança de Rede

A criptografia é a ferramenta mais importante para protecção das redes e das comunicações. As duas formas de criptografia mais utilizadas são: a criptografia convencional ou simétrica e a criptografia de chave pública ou assimétrica [NSEAS00, RSALFAQ00].

2.2.1 Criptografia Convencional ou Simétrica

A criptografia convencional, também designada por criptografia simétrica ou de chave única era o único tipo de criptografia em utilização antes do desenvolvimento da criptografia de chave pública (no final dos anos 70) [NSEAS00, UPKICSDC99].

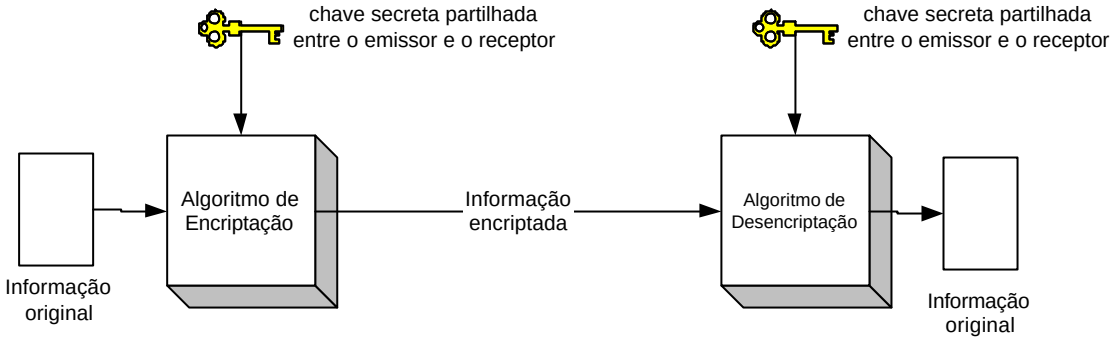


Figura 2.3 Criptografia convencional ou simétrica

Este tipo de criptografia possui os seguintes componentes (Figura 2.3):

- **Informação original**: são os dados originais que servem como entrada para o algoritmo;
- **Algoritmo de Encriptação**: o algoritmo que realiza várias substituições e transformações sobre a informação original;
- **Chave secreta**: a chave que é igualmente fornecida como entrada ao algoritmo. As substituições e permutações realizadas pelo algoritmo dependem da chave;
- **Informação encriptada**: é a mensagem encriptada produzida como resultado da transformação. Depende da informação original e da chave secreta. Para uma determinada mensagem, duas chaves diferentes produzem duas mensagens encriptadas diferentes;
- **Algoritmo de Desencriptação**: é o algoritmo de encriptação a funcionar de forma inversa. Usa a informação encriptada e a chave secreta para produzir a informação original.

A segurança deste tipo de encriptação depende fundamentalmente da manutenção da chave secreta que é utilizada no algoritmo. É assumido que é extremamente difícil desencriptar uma mensagem com base nos dados encriptados e no conhecimento do algoritmo de encriptação/desencriptação – não é necessário manter o algoritmo secreto, basta apenas manter a chave secreta (no Anexo F, Tabela F.1 pode ser consultada uma tabela com alguns dos principais algoritmos de criptografia simétrica) [NSEAS00, RSALFAQ00].

Um dos algoritmos de criptografia convencional mais utilizados actualmente é o DES que foi adoptado inicialmente em 1975 pelo *National Bureau of Standards*. O DES funciona com cifra de bloco que processa a entrada da informação original em blocos de tamanho fixo e produz um bloco de informação encriptada de igual dimensão ao do bloco de informação original.

Neste algoritmo o bloco de texto simples possui uma dimensão de 64 bits e uma chave de 56 bits de dimensão. O texto com mais de 64 bits de dimensão é dividido em blocos de 64 bits de dimensão [WSCRTS97, NSEAS00].

As principais preocupações sobre a segurança do DES resumem-se em dois aspectos fundamentais: o algoritmo em si e o tamanho das chaves utilizadas.

Enquanto que o primeiro se refere ao facto da criptanálise poder explorar as características do algoritmo DES, o segundo traduz uma preocupação mais séria no que diz respeito ao tamanho da chave, e ao facto desta poder ser descoberta através de um ataque de força bruta procurando o espaço total de chaves (2^{56} combinações de chaves possíveis) e encontrando a chave correcta. Com o aumento do poder computacional, o tempo e o custo para encontrar a chave secreta diminuíram, colocando assim em risco a segurança do próprio algoritmo [NSEAS00, RSALFAQ00].

Com base nestas duas preocupações, o DES vai ser substituído pelo AES (*Advanced Encryption Standard*) [AESPRIJ99] que é considerado como um algoritmo mais seguro e flexível que o primeiro [NSEAS00, ICAPKC96].

2.2.2 Criptografia de Chave Pública ou Assimétrica

Igualmente importante como a criptografia convencional ou simétrica é a criptografia de chave pública. Este tipo de criptografia é utilizado fundamentalmente para autenticação de mensagens e distribuição de chaves.

A criptografia de chave pública foi inicialmente proposta por *Diffie* e *Hellman* em 1976 e representou o primeiro verdadeiro avanço na criptografia nos últimos anos. Os algoritmos de chave pública são baseados em funções matemáticas, ao invés de operações sobre *bits*, e são assimétricos, envolvendo a utilização de duas chaves separadas, por oposição à criptografia simétrica convencional [UPKICSDC99]. Este tipo de criptografia possui os seguintes componentes (Figura 2.4 e Figura 2.5):

- **Dados originais**: a mensagem em formato legível ou dados que são utilizados para fornecer ao algoritmo;
- **Algoritmo de Encriptação**: o algoritmo que realiza diversas transformações sobre a informação original;
- **Chave Pública** e **Chave Privada**: este é o par de chaves seleccionado em que uma é utilizada para encriptação e a outra é utilizada para desencriptação. As transformações realizadas pelo algoritmo de encriptação dependem da chave pública ou privada fornecida como entrada para o algoritmo;
- **Dados encriptados**: corresponde à mensagem encriptada produzida como resultado do algoritmo. Depende dos dados originais e da chave. Para uma determinada mensagem, duas chaves diferentes produzem dois textos encriptados diferentes;
- **Algoritmo de Desencriptação**: o algoritmo aceita o texto encriptado e a chave correspondente e produz os dados originais.

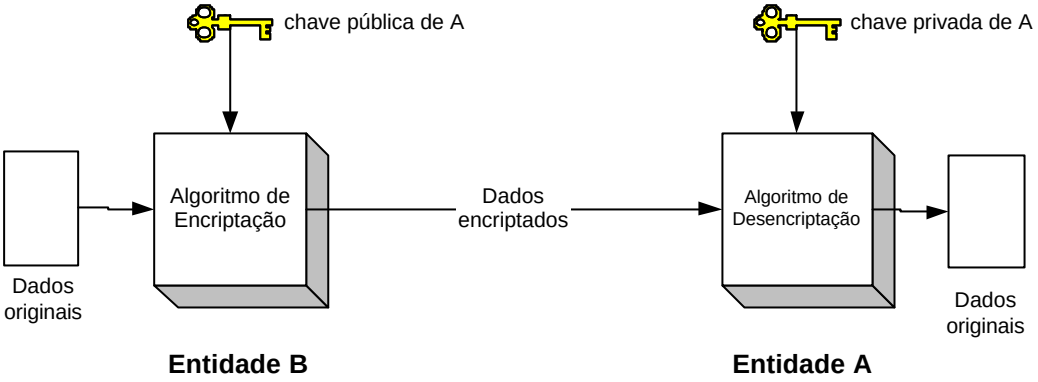


Figura 2.4 Criptografia Assimétrica utilizada para Encriptação

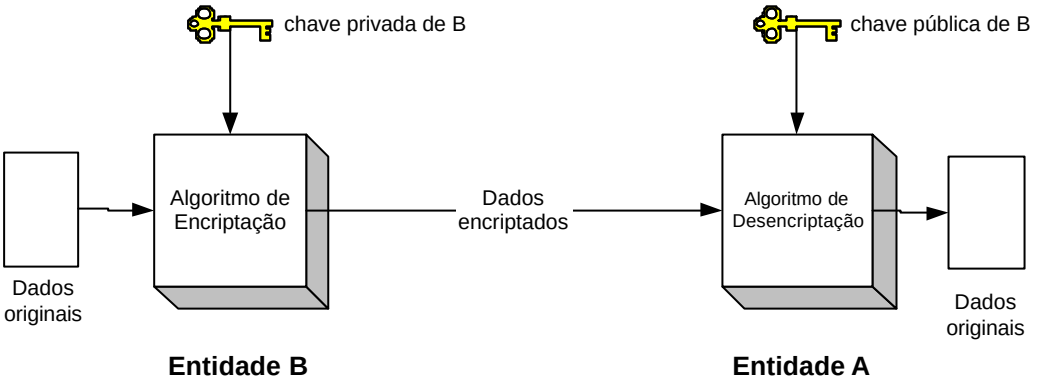


Figura 2.5 Criptografia Assimétrica utilizada para Autenticação

A utilização de duas chaves tem impactos profundos nas áreas da confidencialidade, distribuição de chaves e autenticação. Enquanto que a chave pública do par de chaves correspondente é publicada para todos que a desejem utilizar, a chave privada é conhecida apenas pelo detentor da mesma [NSEAS00, RSALFAQ00]. Um algoritmo de criptografia de chave pública depende de uma chave para encriptação e da outra chave correspondente para desencriptação (no Anexo F, Tabela F.2 pode ser consultada uma tabela com alguns dos principais algoritmos de criptografia assimétrica e as suas aplicações).

O processo desenrola-se da seguinte forma:

- Cada utilizador gera um par de chaves que será utilizado para encriptar e desencriptar as mensagens;
- Cada utilizador coloca uma das suas duas chaves num registo público: a chave pública. A outra chave é mantida secreta;
- Caso um utilizador B deseje enviar uma mensagem privada para um utilizador A, B deve encriptar a mensagem utilizando a chave pública de A;
- Quando A recebe a mensagem, desencripta-a utilizando a sua correspondente chave privada.

O primeiro algoritmo/protocolo de chave pública foi criado por *Diffie* e *Hellman* em 1976. O objectivo deste foi o de permitir que dois utilizadores pudessem trocar uma chave secreta entre si de uma forma secreta, que pode depois ser utilizada para encriptar as mensagens subsequentes, trocadas entre ambos [NSEAS00,

WSCRTS97]. Uma descrição detalhada de como o algoritmo funciona pode ser encontrada no Anexo F, Tabela F.3.

Igualmente, um dos primeiros algoritmos de chave pública - RSA - foi desenvolvido em 1977 por *Ron Rivest*, *Adi Shamir* e *Len Adleman* no MIT e foi publicado em 1978. Desde então assumiu-se como o principal algoritmo de encriptação de chave pública que maior aceitação e utilização tem tido a nível mundial [WSCRTS97]. Uma descrição detalhada de como funciona pode ser encontrada no Anexo F, Tabela F.4.

2.2.3 Autenticação

Enquanto que a criptografia oferece protecção contra ataques passivos (visualização não autorizada de informação), a autenticação oferece protecção contra ataques activos (falsificação de dados e de transacções). Por definição, uma mensagem, um ficheiro ou outro qualquer dado é autêntico quando este é genuíno e é proveniente de uma fonte de informação esperada [PKIIMES01].

A autenticação depende e pode ser categorizada por um ou mais dos seguintes três factores (Tabela 2.1):

- Factor Conhecimento: “algo que se sabe”;
- Factor Posse: “algo que se possui”;
- Factor Biométrico: “característica que se possui”.

Factor conhecimento	Algo que apenas o utilizador sabe	Uma palavra-chave ou código PIN; Informação acerca do utilizador ou membros da sua família; Respostas secretas a perguntas pré-estabelecidas.
Factor Posse	Algo que apenas o utilizador possui	Chave física; Cartão de fita magnética; Cartões Inteligentes.
Factor Biométrico	Característica que apenas o utilizador possui	Impressão digital; Íris ocular; Geometria da mão; Reconhecimento de voz.

Tabela 2.1 Tipos de Autenticação

Todos os mecanismos de autenticação oferecem, como funcionalidade básica, uma forma de autenticação unidireccional, em que apenas uma das entidades se autentica a outra. Apenas alguns dos mecanismos de autenticação oferecem autenticação mútua, em que ambas as entidades se autenticam uma face à outra. A autenticação baseada em PKI pode oferecer ambos [PPKI01]. Os diversos mecanismos de autenticação existentes são:

Autenticação com Palavra-chave

Quase todos os sistemas informáticos solicitam que os utilizadores se identifiquem ao iniciar uma sessão, através da utilização de um nome de utilizador e de uma palavra-chave (Figura 2.6). Esta palavra-chave é um segredo que é partilhado pelo utilizador e pelo recurso a que este se está a tentar identificar. A

autenticação baseada em palavra-chave é a forma mais simples de autenticação embora seja igualmente mais fraca estando sujeita ser sujeita a diversos tipos de ataque (um destes ataques designa-se por *sniffing*) [PKIWTB01, PPKI01].

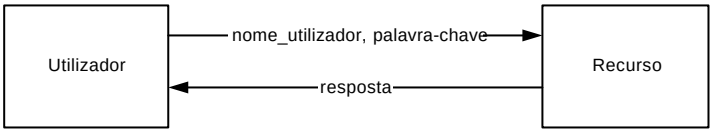


Figura 2.6 Exemplo de autenticação com palavra-chave

Autenticação com valores de utilização única (*One-Time*)

Este tipo de autenticação é uma evolução da anterior, utilizando um valor secreto de cada vez que ocorre um pedido de autenticação. Existem três subtipos neste grupo: desafio/resposta, desafio implícito e autenticação baseadas em *hash*. De seguida, cada um deles é apresentado com mais detalhes.

Desafio/Resposta

Neste tipo de autenticação, o recurso em que o utilizador se deseja autenticar gera um desafio aleatório que é enviado para o utilizador. O utilizador encripta esse desafio com uma chave conhecida apenas pelo utilizador e pelo recurso (Figura 2.7). O recurso desencripta esses dados e compara o desafio enviado pelo utilizador com o original enviado por si. Se ambos forem idênticos a autenticação é bem sucedida. Neste tipo de autenticação o recurso e o utilizador devem estabelecer *a priori* quais as chaves que vão ser utilizadas [PPKI01, NSEAS00].

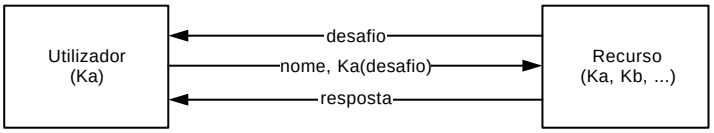


Figura 2.7 Exemplo de autenticação com Desafio-Resposta

Baseado em Data/Hora

Neste tipo de autenticação o utilizador que se pretende autenticar ao recurso, lê o valor do relógio do seu sistema informático e encripta-o com uma chave conhecida pelo utilizador e pelo recurso. O recurso desencripta esses dados e compara-os com o valor do relógio do seu próprio computador [NSEAS00, RSALFAQ00]. No caso dos valores serem suficientemente próximos a autenticação é bem sucedida (Figura 2.8).

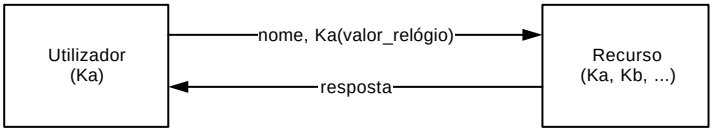


Figura 2.8 Exemplo de autenticação baseado na Data/Hora

Baseado em *Hash*

Este método de autenticação baseia-se numa sequência de palavras-chave que são geradas através da aplicação sucessiva de uma função de *hash*. O valor do *hash* inicial é calculado através do *hash* de uma palavra-chave secreta do utilizador concatenada com um outro valor não secreto

(designado por semente). O primeiro valor do *hash*, que é resultado da primeira aplicação da função de *hash*, torna-se a entrada da segunda aplicação da função de *hash*, e assim sucessivamente (Figura 2.9).

É necessário, no entanto, um passo inicial para inicializar o recurso a que se deseja aceder: o utilizador deve enviar a palavra-chave inicial, um número sequencial e uma semente [NSEAS00, RSALFAQ00].

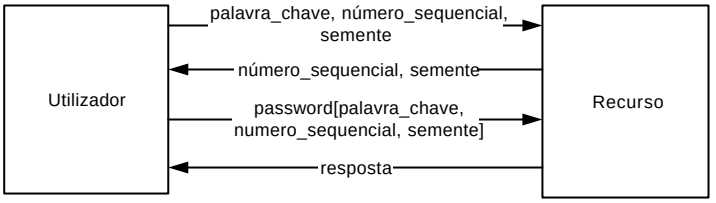
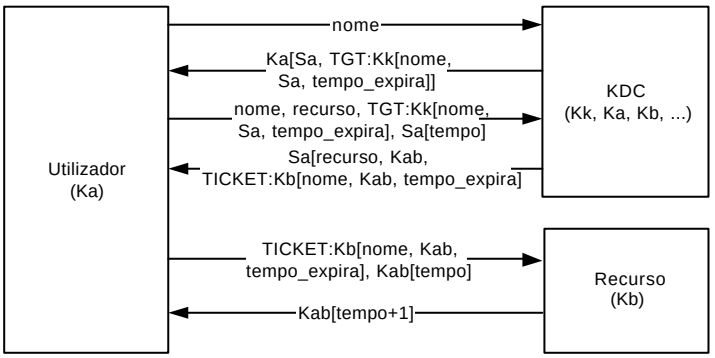


Figura 2.9 Exemplo de Autenticação baseado em *Hash*

Autenticação com *Kerberos*

O MIT desenvolveu um mecanismo de autenticação baseado em criptografia designado por *Kerberos*. Esta designação teve a sua origem no nome de um cão de três cabeças da mitologia grega que guardava a entrada para o Hades (Inferno). Esta metodologia de autenticação envolve três partes distintas: o utilizador, o recurso ao qual o utilizador se deseja autenticar e um Centro Distribuidor de Chaves (KDC[9]) [NSEAS00, PPK01]. O KDC fornece ao utilizador os recursos necessários (bilhete de autorização) para que este se possa autenticar face ao recurso desejado (Figura 2.10).



Ka	Chave mestre do utilizador; conhecida pelo utilizador e pelo KDC
Kb	Chave mestre do Recurso; conhecida pelo Recurso e pelo KDC
Kab	Chave de sessão para o utilizador e para o Recurso; conhecida pelo utilizador, pelo Recurso e pelo KDC
Kk	Chave mestre do KDC; conhecido pelo KDC
Sa	Chave de sessão do login do utilizador; conhecida pelo utilizador e pelo KDC

Figura 2.10 Exemplo de Autenticação baseado em *Kerberos*

Autenticação baseada em Certificados

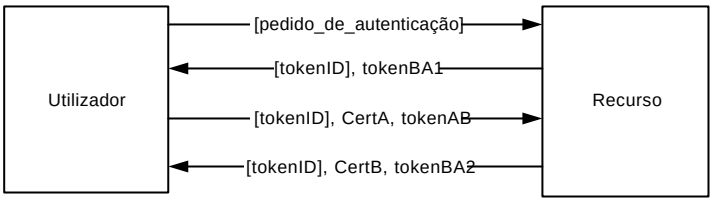
No caso de um utilizador possuir um certificado, a confiança num KDC pode ser removida. Isto não remove, no entanto, a necessidade de confiança em entidades terceiras, uma vez que uma Autoridade de Certificação (CA[10]) assume este papel [NSEAS00, RSALFAQ00]. Apesar disto, e ao contrário do que

[9] Key Distribution Center

[10] *Certification Authority*

acontece com o KDC, no caso da CA não estar disponível a autenticação pode ser conseguida com sucesso (Figura 2.11).

Alguns dos protocolos mais utilizados nos nossos dias oferecem este tipo de autenticação: SSL/TLS, SET, Internet *Key Exchange* (IKE), entre outros.



[pedido_de_autenticação]	Opcional. O utilizador solicita ao servidor que inicie a autenticação
[tokenID]	Opcional. Identifica o tipo de autenticação, versão do protocolo e unidade do protocolo.
CertA	Certificado do utilizador
CertB	Certificado do recurso
tokenBA1	Número aleatório gerado pelo recurso (randB)
tokenAB	randA, randB e nameB assinados pelo utilizador. randA é um número aleatório gerado pelo utilizador; randB é repetido do tokenBA1; e o nome é o nome do recurso
tokenBA2	randA, randB, e nomeA assinados pelo recurso. randA é repetido do tokenAB; randB é repetido do tokenAB e tokenBA1; nomeA é o nome do utilizador.

Figura 2.11 Exemplo de Autenticação baseado em Certificados

Os mecanismos de autenticação baseados em certificados digitais permitem elevar a criptografia de chave pública ao encontro dos requisitos necessários para a existência de autenticação num ambiente distribuído.

Autenticação utilizando Criptografia Convencional

Através da utilização de criptografia convencional é possível proceder à autenticação, se se assumir que ambos o emissor e receptor partilham uma chave secreta comum. Neste caso, apenas o emissor original poderia encriptar a mensagem com sucesso para o receptor. Se esta mensagem incluir um número sequencial, o receptor assegura-se que não existiram alterações e que a sequência é a adequada. A mensagem pode ainda incluir um *timestamp*, o que assegura ao receptor que esta não sofreu atrasos significativos que não sejam originários do trânsito em rede, ou que não foi sujeito ao ataques "por repetição" [NSEAS00, RSALFAQ00].

Código de Autenticação de Mensagens (MAC[11])

Uma das técnicas de autenticação envolve a utilização de uma chave secreta para gerar um pequeno bloco de dados, designado por Código de Autenticação de Mensagens (MAC), que é acrescentado à mensagem original. Esta técnica assume que duas partes em comunicação, A e B, partilham uma chave secreta $K_{A,B}$. Quando A tem uma mensagem e enviar a B, calcula o MAC como função da mensagem e da chave: $MAC_M=F(K_{AB}, M)$. A mensagem e o código são transmitidos para o receptor (Figura 2.12). O receptor efectua o mesmo cálculo sobre a mensagem recebida, utilizando a mesma chave, gerando um novo MAC ($MAC_{M'}$). O código MAC recebido é comparado com o código gerado e caso esta seja igual o receptor é assegurado que a mensagem não foi alterada e que a mensagem é proveniente do emissor correcto [NSEAS00, AIAAD00].

[11] MAC – Message Authentication Code

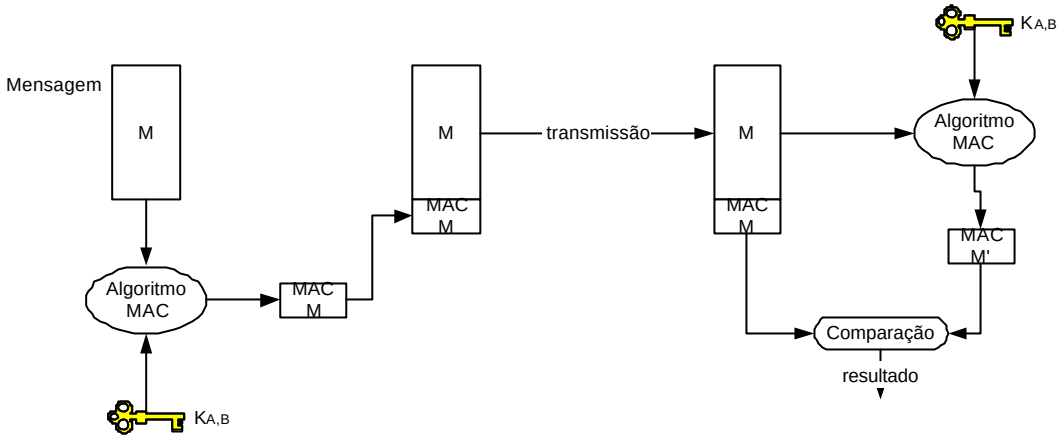


Figura 2.12 Utilização de Autenticação de Mensagens

2.2.4 Função de *Hash* de um só sentido

Uma variante ao MAC consiste na utilização de uma função de *hash* de um só sentido. Esta função aceita uma mensagem M de tamanho variável como entrada e produz um bloco de dados de tamanho fixo (resumo) H(M) como resultado. Ao contrário do MAC não necessita de utilizar uma chave secreta e o resumo é enviado com a mensagem original. Para evitar ataques de modificação do resumo é conveniente utilizá-lo em conjunto com a criptografia: convencional (Figura 2.13) ou de chave pública (Figura 2.14).

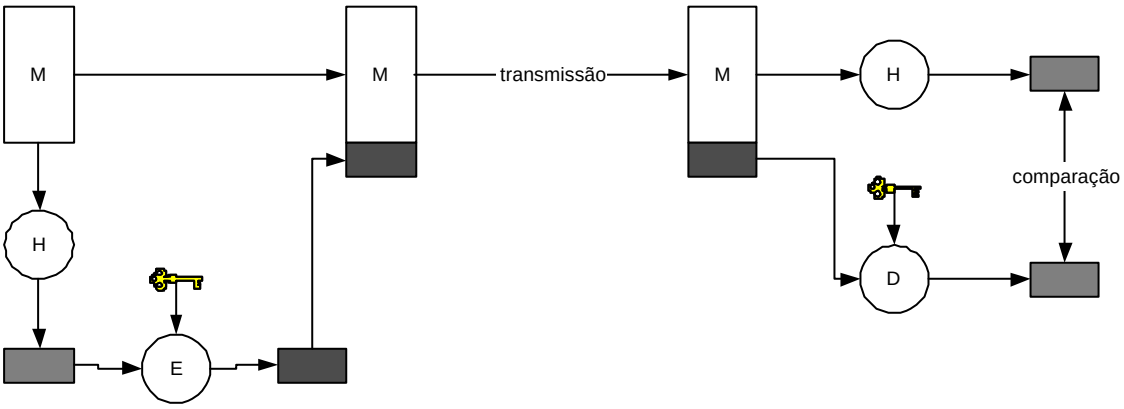


Figura 2.13 Utilizando a criptografia convencional

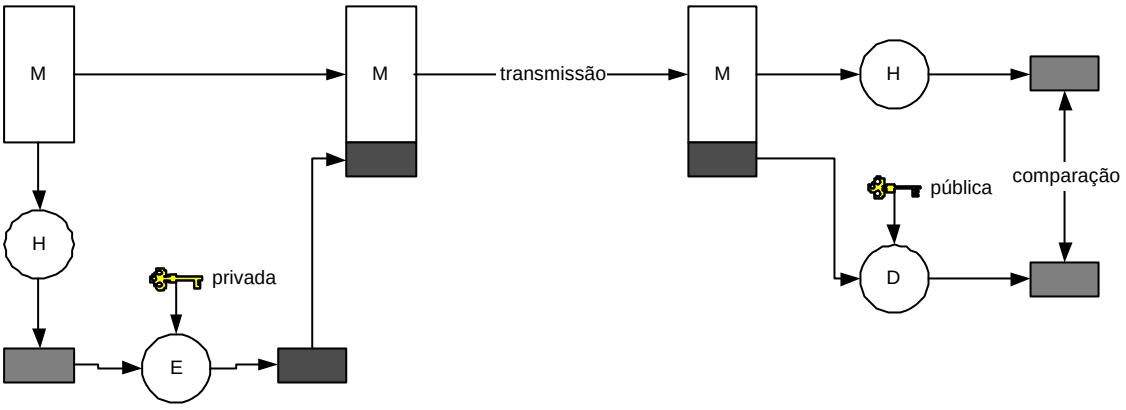


Figura 2.14 Utilizando a criptografia de chave pública

Estas funções de *hash* de sentido único ou função de *hash* seguro são utilizadas não apenas para autenticação de mensagens mas também para assinaturas digitais [NSEAS00, RSALFAQ00]. Algumas das propriedades destes algoritmos são:

- H pode ser aplicada a um bloco de dados de qualquer tamanho;
- H produz um resultado de tamanho fixo;
- H(x) é fácil de calcular quer em implementações de *hardware* quer em *software*;
- Para qualquer código h é impossível calcular um x tal que H(x)=h;
- Para qualquer código x, é impossível achar um y≠x em que o H(y)=H(x);
- É igualmente impossível encontrar um par (x,y) tal que H(x)=H(y).

Alguns dos algoritmos mais importantes de *hash* existentes são os seguintes: SHA-1, MD5, RIPEMD-160 e HMAC.

2.2.5 Assinaturas Digitais

A criptografia de chave pública pode ser igualmente utilizada para autenticação para além da encriptação. Se uma entidade 'B' desejar enviar uma mensagem para uma entidade 'A', para que 'A' tenha a certeza de que a mensagem provém efectivamente de 'B' e não de outrém, 'B' utiliza a sua chave privada e encripta a mensagem. Quando 'A' a recebe e a desencripta com a chave pública de 'B' pode ter a certeza que esta foi efectivamente encriptada por este. Esta mensagem, encriptada desta forma, serve como assinatura digital.

Existe uma forma de assinatura digital mais eficiente, que se baseia na combinação de funções de *hash* com a criptografia de chave pública. Assim, 'B' pode utilizar uma função de *hash* para gerar um valor numérico da mensagem original e encriptá-lo com a sua chave privada. Esta informação designa-se por assinatura digital. A entidade 'A' recebe a mensagem original em conjunto com a assinatura digital da mesma. A entidade 'A' desencripta o valor numérico enviado, utilizando a chave pública de IBM, e calcula o *hash* da mensagem

original. A entidade DAT compara os dois valores numéricos obtidos e verifica a sua igualdade, verificando assim a assinatura digital de IBM [NSEAS00, UPKICSDC99].

No exemplo acima citado, a mensagem por si só não está protegida, mas através da combinação de chaves é possível assegurar, quer a sua protecção, quer a sua autenticidade, conforme se pode verificar na figura seguinte (Figura 2.15):

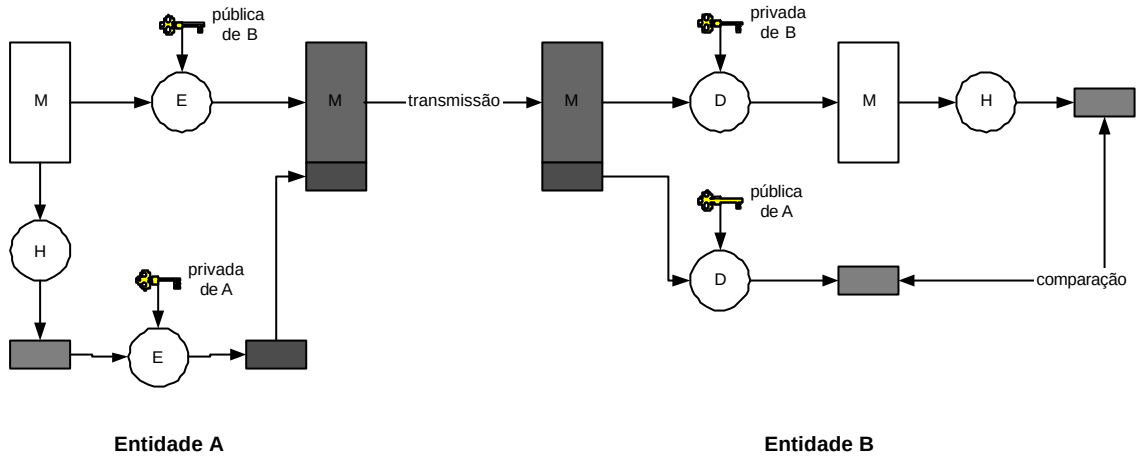


Figura 2.15 Assinaturas Digitais

Um caso particular das assinaturas digitais é a assinatura digital cega. Tal como qualquer assinatura digital, apenas a entidade que assina pode criar a assinatura utilizando a sua chave privada, enquanto que qualquer um pode verificar a assinatura usando a sua chave pública. No entanto, e ao contrário do que ocorre no processo de assinatura digital normal, a entidade que assina não tem conhecimento do conteúdo da mensagens que está a assinar nem que assinatura digital está a criar [NSEAS00, RSALFAQ00]. Um dos protocolos mais utilizados para este tipo de assinaturas é o Protocolo de Assinaturas Digitais Cegas de *Chaum* (Anexo F, Tabela F.5).

2.2.6 Certificados Digitais

Um dos problemas base da criptografia de chave pública consiste na determinação do correspondente detentor da chave privada. Para poder responder a esta questão as PKI dependem do conceito de certificado digital de chave pública. Um certificado digital é o elemento mais básico de uma PKI. Cada certificado contém a chave pública que identifica o utilizador detentor da correspondente chave privada.

Os certificados digitais não são um conceito muito inovador e na verdade apresentam semelhanças com alguns dos instrumentos de identificação que são utilizados no nosso dia a dia: bilhete de identidade, cartão pessoal ou de empresa, cartão de crédito, são apenas alguns destes instrumentos [PPKI01, TPKIRRR99].

Um certificado digital é um documento electrónico que contém a chave pública de uma entidade e um identificador único da mesma. Os certificados são emitidos por entidades terceiras de confiança tais como governos ou instituições financeiras. Estas entidades designam-se por Autoridades de Certificação (CA). Antes da emissão de um certificado a CA assina-o digitalmente usando a sua própria chave privada. Todos os restantes participantes podem confiar no conteúdo do certificado uma vez que devem usar a chave pública da CA em que confiam para verificar a assinatura digital do certificado. Uma outra definição de

certificado, que é muitas vezes apresentada, consiste em defini-lo como um documento electrónico emitido por uma entidade terceira, que serve como prova física da identidade e/ou privilégio do detentor. Um certificado contém tipicamente tanto a chave pública do sujeito a ser certificado (conjuntamente com informação que o identifica), como um identificador único [OFPKI00].

O certificado ideal deveria combinar todas as características dos instrumentos de identificação referidos anteriormente, assim como algumas importantes características adicionais [PPKI01, PKIWTB01], nomeadamente:

- Dever ser um objecto puramente digital, de forma a poder ser distribuído através da Internet (ou outro meio de comunicação digital) e processado de uma forma automática;
- Dever conter o nome do utilizador detentor da chave privada, identificando a organização deste e incluir informação de contacto;
- Dever ser fácil verificar se foi ou não emitido recentemente;
- Dever ser criado por uma entidade terceira de confiança em vez de ser criado pelo utilizador que detém a chave privada;
- Uma vez que a entidade terceira de confiança pode criar inúmeros certificados (inclusive para um único utilizador) estes deveriam ser facilmente distinguidos entre si;
- Dever ser possível verificar se é real ou se foi falsificado;
- Dever ter uma protecção contra alterações para que não seja possível alterar o seu conteúdo;
- Dever ser possível verificar de imediato se a informação de um certificado é válida ou não;
- Dever ser possível verificar no certificado para que aplicação é que este se destina.

São diversas as aplicações dos certificados, das quais se podem destacar:

- Estabelecimento de ligações seguras através da Internet/Intranet;
- Autenticação de clientes Web;
- Encriptação e assinatura de correio electrónico;
- Publicação de software;
- Entre outras.

Actualmente existe uma aproximação ao certificado ideal cujas características se assemelham às apresentadas anteriormente. Designa-se por certificado de chave pública, e é um objecto puramente digital.

Um certificado de chave pública para além de conter informação acerca da entidade que está a ser certificada, assim como da sua chave pública, pode ainda conter informação da organização a que pertence a entidade a ser certificada, informação de contacto, entre outras. Contém igualmente informação acerca da validade do mesmo e ainda informação acerca da entidade que o emitiu. Finalmente todo o conteúdo do certificado está protegido com a assinatura da entidade emissora [PPKI01, UPKICSDC99].

Em termos de tipologia de certificados digitais (Tabela 2.2), existem três tipos principais [PPKI01]:

- **Certificados de Identidade**: um certificado de identificação é aquele que contém uma chave de verificação de assinaturas combinada com informação suficiente para permitir identificar (espera-se que, de uma forma única) o detentor da chave;
- **Certificados de Acreditação**: este tipo de certificado identifica o detentor da chave como sendo parte de um determinado grupo ou organização sem ter que revelar a sua identidade. Em diversas circunstâncias, uma assinatura digital é necessária para autorizar uma determinada transacção mas a identidade do detentor da chave não é relevante. Este tipo de certificados pode ser igualmente visto como um certificado de autorização ou permissão. No entanto, enquanto que este certificado não pode conter dados de identificação do detentor da chave, o emissor do mesmo terá esta informação;
- **Certificados de Autorização e de Permissões**: nestes tipos de certificados, a autoridade que emite o certificado delega alguma forma de autorização à chave assinada. Em geral, o detentor de qualquer recurso que envolva acesso electrónico pode utilizar um certificado de autorização para controlar o acesso ao mesmo. Embora os certificados de autorização possam conter informação acerca da identificação, esta não é em geral necessária e por vezes até se torna indesejável [IDCWH98].

Tipo de certificado	Requisitante	Emissor	Verificador
Identidade	A pessoa em questão	Uma agência apropriada	Alguém responsável por efectuar uma validação da identidade
Acreditação	Um membro qualificado	A entidade profissional	Um utilizador dos serviços oferecidos por um membro
Autorização ou Permissão	Um cliente que deseje aceder a um recurso	O dono do recurso	O dono do recurso

Tabela 2.2 Tipos de certificados digitais

Em termos práticos, um certificado digital é utilizado para relacionar o nome de uma determinada entidade (e possivelmente outros atributos relacionados com essa mesma entidade) com a sua correspondente chave pública. Quando se discute o conceito de certificado é importante assinalar a existência de diferentes tipos e formatos de certificados, nomeadamente:

- Certificados de Chave Pública X.509 (X.509);
- Certificados de Infra-estrutura de Chave Pública simples (SPKI);
- Certificados de *Pretty Good Privacy* (PGP);

2.2.6.1 Certificados de Chave Pública X.509

O X.509 é uma norma ITU-T[12] para a definição do formato de um certificado digital. Definido no contexto das normas ISO[13] e ITU-T relacionados com os serviços de Directoria, o X.509 é a norma fundamental que serve como base à definição da estrutura dos certificados de chave pública. Foi publicado pela primeira vez em 1988, tendo sido revisto em 1993 e em 1996. A versão actual é a 3 (X.509v3) e inclui suporte para extensões que lhe conferem alguma flexibilidade. Um certificado X.509v3 inclui uma série de campos obrigatórios de uma forma pré-determinada e um conjunto opcional de extensões [UPKICSDC99].

O X.509 define o formato de um certificado emitido por uma Autoridade de Certificação (CA) para uma entidade (A), representado simbolicamente como [OCX509CA98]:

$$CA\langle\langle A\rangle\rangle = CA\{V, SN, AI, CA, [UCA], A, [UA], Ap, T^A, [Ext]\}$$

Em que:

V: o número de versão do certificado (1, 2 ou 3);

SN: o número de série do certificado;

AI: identifica o algoritmo de assinatura usado para assinar o certificado;

CA: o nome distinto da CA emissora;

UCA: o identificador único da CA (opcional);

A: o nome distinto do sujeito identificado pelo certificado;

UA: o identificador único do sujeito (opcional);

Ap: a chave pública do sujeito A;

T^A: o período de validade do certificado descrito por uma data de início e de fim durante a qual o certificado é válido;

Ext: define um conjunto de extensões que permitem a inclusão de informação adicional no certificado sem alterar o seu formato (opcional).

O serviço de Directoria X.500 no qual se baseia o X.509, requer uma autenticação forte que assegure que apenas os utilizadores devidamente autorizados podem efectuar alterações. Quando a Directoria contém informação confidencial a autenticação pode ser utilizada para controlar o acesso à mesma.

Ao longo da sua evolução, o X.509, cujo enfoque inicial tinha sido o suporte ao serviço de Directoria X.500, alterou o seu desenvolvimento no sentido de contribuir para a criação de uma PKI genérica.

Os certificados X.509 podem ser considerados como sendo o conjunto de três componentes interligadas: (1) o envelope com evidência da confiança, (2) conteúdo do certificado e (3) um conjunto opcional de extensões (Figura 2.16).

[12] ITU-T: International Telecommunications Union-Telecommunications

[13] ISO: International Standards Organization

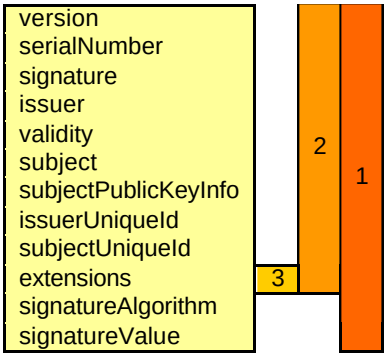


Figura 2.16 Conteúdo de um Certificado Digital X.509

O ASN.1 ou *Abstract Syntax Notation One* é um método de especificação de objectos abstractos, que foi definido na norma X208. O ASN.1 é uma notação flexível que permite a definição uma variedade de tipos de dados, desde dados mais simples até estruturas mais complexas. Os certificados X.509 são representados em ASN.1 e podem depois ser convertidos para um formato binário mais adequado para circulação numa rede de comunicações e para armazenamento. A norma X.209 define um conjunto de regras de codificação ASN.1 designadas por BER – *Basic Encoding Rules*. Outra forma de codificação designa-se por DER – *Distinguished Encoding Rules* e representa um subconjunto das regras de codificação BER [UPKICSDC99, PPKI01].

O BER permite codificar um determinado valor ASN.1 como um conjunto de *bytes* de três formas distintas dependendo do tipo e o tamanho do valor. O DER é um subconjunto do BER e permite codificar de uma forma única um valor ASN.1 sendo usado para aplicações em que é necessário um valor único de um conjunto de *bytes*.

De forma a identificar o sujeito no certificado e a entidade emissora do certificado, o X.509 depende de uma estrutura de informação que suporta um sistema de nomes hierárquicos designado por *Distinguished Name* (DN). O objectivo do conjunto de especificações X.500 era a definição uma Directoria Global e como tal necessitava de uma forma de identificar univocamente todas as entidades que dela fizessem parte, utilizando para isso o DN. No entanto, os mecanismos de DNs não foram muito bem sucedidos devido a:

- O conceito de DN nunca foi muito bem aceite entre a comunidade de utilizadores em geral, devido ao pouco sucesso do X.500 e da crescente utilização do endereço de correio electrónico como forma universal de identificação;
- Por outro lado, uma autoridade responsável por atribuir DNs nunca existiu [PPKI01, WICHTIL98].

Um certificado X.509 e as suas correspondentes extensões são definidos recorrendo aos tipos ASN.1. No seu nível mais extenso e global, os certificados X.509 possuem três campos principais: (a) o certificado a ser assinado, o (b) identificador do algoritmo de assinatura e o (c) valor da assinatura.

(a) *tbsCertificate*: contém o conteúdo do certificado assinado;

(b) *signatureAlgorithm*: contém o identificador do algoritmo de assinatura digital;

(c) *signatureValue*: contém a assinatura digital.

A parte do certificado a ser assinada (*tbsCertificate*) contém uma série de informação que constitui o conteúdo do próprio certificado [UPKICSDC99]:

- *version*: indica a versão do certificado;
- *serialNumber*: indica o número de série atribuído pela entidade emissora do certificado;
- *signature*: contém o identificador do algoritmo de assinatura;
- *issuer*: este campo contém o nome distinto (DN) X.500 do emissor do certificado;
- *validity*: contém dois componentes (uma data de inicio e uma data de fim) que indicam a validade do certificado;
- *subject*: contém o nome distinto (DN) X.500 do detentor da chave privada correspondente à chave pública neste certificado;
- *subjectPublicKeyInfo*: contém a chave pública do sujeito e o identificador do algoritmo;
- *issuerUniqueId* e *subjectUniqueId*: são identificadores que identificam o emissor do certificado e o sujeito a ser certificado;
- *extensions*: este campo opcional contém uma ou mais extensões em que cada extensão possui um identificador, um indicador de importância e um valor da extensão.

No entanto, com o desenvolvimento das PKI, ficou demonstrado que o conteúdo original dos certificados X.509 era insuficiente. Foi a partir desta limitação que foram sendo criadas extensões nos certificados, permitindo que uma CA pudesse incluir informação não suportada pelo formato básico do certificado. As extensões possuem três componentes principais: um identificador de extensão, um identificador de importância e o valor da extensão. O ITU-T e o IETF definiram um conjunto de extensões para os certificados X.509 versão 3 que podem ser encontradas na especificação X.509 [OCSX509CA98, PPKI01].

2.2.6.2 Certificados SPKI

O SPKI pretendia fornecer os mecanismos necessários para suportar a segurança num número bastante variado de aplicações de Internet, incluindo protocolos IPSec, correio electrónico encriptado, documentos de WWW, protocolos de pagamento e muitas outras aplicações em que seja necessária a utilização de certificados digitais e a possibilidade de acesso aos mesmos. O SPKI pretendia igualmente suportar uma grande variedade de modelos de confiança [SPKC98].

O grupo de trabalho do SPKI definiu uma nova forma normalizada para certificados digitais, designada SPKI, cujo princípio fundamental é a autorização ao invés da autenticação. Estes certificados ligam os nomes ou autorizações a chaves ou outros objectos. Esta ligação pode ser obtida directamente através de uma chave explícita, ou indirectamente através do *hash* de uma chave. As estruturas de informação que são utilizadas para conter a informação deste tipo de certificados utilizam uma representação com formato canónico, designado por *S-Expression* (Expressão-S).

Para perceber um pouco melhor o conceito que está por detrás do SPKI algumas definições são importantes. Algumas destas definições são comuns à maior parte de outros formatos de certificados:

- **Principal**: um Principal corresponde a uma chave criptográfica, capaz de gerar uma assinatura digital.

- ***S-Expression***: uma *S-Expression* é o formato de dados que foi escolhido pelo SPKI e pelo SDSI. Estas expressões assumem um formato semelhante a expressões limitadas por parêntesis, tal como o LISP, com a limitação de que listas vazias não são válidas e o primeiro elemento de uma *S-Expression* que deve ser uma cadeia de caracteres (o tipo da expressão).

- **Formato canónico**: uma *S-Expression* canónica contém cadeias de caracteres, cada uma com um determinado tamanho e pontuação "()[]" para formar listas.

A equipa que desenvolve o SPKI abordou o problema existente na ligação entre <nome, chave> e depressa se apercebeu que este tipo de certificados era de utilização limitada na gestão da confiança. Por forma tentar resolver este tipo de problemas nasceu então o SPKI [SPKICT98].

Os conceitos principais de um certificado SPKI residem na autorização de uma determinada acção, na atribuição de permissões e na atribuição de determinadas capacidades a um detentor de uma chave.

Um certificado SPKI define uma autorização linear da seguinte forma: autorização => chave. No caso de alguém desejar aceder ao nome do detentor de uma chave é possível estabelecer a ligação entre uma chave e a localização da informação: autorização => chave => nome.

Um certificado SPKI é o mais simples possível. É necessário um conjunto mínimo de campos para representar toda a informação do certificado, e os campos opcionais são também reduzidos ao mínimo. Não são necessárias quaisquer bibliotecas de código externas para empacotar ou processar os certificados SPKI. O ASN.1 (largamente utilizado no X.509) não é utilizado no SPKI. O ASN.1 é extremamente difícil de processar, e os processadores de ASN.1, são normalmente, programas muito exigentes em termos de memória [SPKIREQ98].

Cada certificado SPKI básico pode ser representado através de um conjunto de cinco elementos, normalmente designados por tuplo-5. Este grupo de cinco tuplos é constituído por: Emissor, Sujeito, Delegação, Autorização, Validação – I,S,D,A,V.

- **Emissor**: uma chave pública, o seu *hash*, ou a palavra reservada '*Self*';

- **Sujeito**: uma chave pública, o seu *hash*, um nome utilizado para identificar a chave pública, ou o *hash* de um objecto;

- **Delegação**: contém um valor booleano, que no caso de ser verdade, o sujeito é permitido pelo emissor a propagar a autorização contida neste certificado;

- **Autorização**: uma *S-Expression* que contém as regras para a combinação da autorização concedida;

- **Validade**: a validade de um certificado SPKI, que contém uma dada e hora de início e de fim para este certificado.

2.2.6.3 Certificados *Pretty Good Privacy* (PGP)

O *Pretty Good Privacy* – PGP é um programa criptográfico criado por *Phill Zimmerman* no inicio dos anos 90 que utiliza algoritmos criptográficos como o RSA e o IDEA (semelhante ao DES) para encriptar e assinar mensagens, e foi criado originalmente para ser utilizado com o correio electrónico baseado na Internet. A versão mais recente do PGP designa-se por OpenPGP e foi publicada numa norma do IETF designada por RFC2440 [RFC2440]. O OpenPGP define um formato de certificados próprio e especifica as regras necessárias para a validação dos mesmos [NAICPGP00].

No PGP, cada um dos utilizadores mantém uma lista própria de chaves públicas dos utilizadores com os quais se correspondem (e confiam), designada por anel de chaves. Como protecção contra ataques maliciosos, o anel de chaves é assinado digitalmente pelo detentor do mesmo com a correspondente chave privada [NAICPGP00].

O PGP permite que os utilizadores possam trocar os seus próprios anéis de chaves entre si. Assim, quando o utilizador introduz a chave pública de outro indivíduo ao seu anel de chaves, atribui-lhe um dos seguintes atributos:

- **Confiança Completa**: se outra chave assinou esta chave, então pode ser adicionada ao anel de chaves;
- **Confiança Marginal**: uma chave assinada por esta chave deve também ser assinada por uma ou várias outras chaves antes de ser adicionada ao anel de chaves;
- **Sem Confiança**: não usar esta chave para determinar se uma chave pode ou não ser adicionada ao anel de chaves;
- **Desconhecido**: o nível de confiança não pode ser determinado para a chave em causa.

À medida que os utilizadores trocam os seus anéis de chaves vão construindo uma rede de confiança entre si. Em muitos aspectos, esta é a forma mais simples de PKI. Cada um dos utilizadores funciona como a sua própria Autoridade de Certificação de topo com autoridade total na determinação de como a chave é assinada. Esta simplicidade de utilização permitiu que o PGP tivesse crescido em termos de utilização quando comparado a outras PKI, no entanto, no caso do Comércio Electrónico ou outras aplicações que necessitem de autenticação forte o PGP falha redondamente [PPKI01].

Um certificado PGP não é extensível e contém apenas um endereço de correio electrónico, uma chave pública e um atributo indicativo do nível de confiança (conforme a lista apresentada acima). Uma vez que um endereço de correio electrónico não é uma forma segura de identificar alguém, o PGP não poderá fornecer o nível de autenticação forte da identidade de uma entidade.

O PGP não possui um método coerente para validação e revogação de certificados e ambas as funções ocorrem normalmente neste sistema por contacto directo e pessoal (quase “boca-a-boca”).

A utilização do endereço de correio electrónico como única forma de identificação das entidades impede que os utilizadores possam beneficiar de algum nível de privacidade. O utilizador pode sempre usar um endereço de correio electrónico fictício, no entanto, isso destruirá qualquer forma de autenticação de confiança [RPKIECCA00].

2.3 Componentes, Serviços e Mecanismos das PKI

Nesta parte do capítulo e conforme tinha sido identificado no início do mesmo, vão ser descritos os diversos componentes, serviços e mecanismos integrantes das PKI.

2.3.1 Componentes das PKI

Conforme o que já foi referido anteriormente, as PKI facilitam a utilização da criptografia de chave pública, através da criação e distribuição de certificados de chave pública e de listas de revogação de certificados. As PKI são construídas com base em diversos componentes, cada um destes concebidos para desempenhar um conjunto de tarefas bem definidas. Assim, os componentes básicos de uma PKI são [UPKICSDC99]:

- Autoridade de Certificação;
- Autoridade de Registo;
- Repositório;
- Arquivo

2.3.1.1 Autoridade de Certificação

A Autoridade de Certificação (CA) é o componente base de uma PKI. A CA é uma colecção de *hardware*, *software* e de pessoas que a operam. Uma CA é representada por dois atributos principais: a sua identificação e a sua chave pública. Esta CA desempenha quatro funções principais [PPKI01]:

- Emissão de Certificados (a sua criação e correspondente assinatura digital);
- Manutenção de informação do estado dos certificados e emissão das listas de Revogação de Certificados (CRL);
- Publicação dos seus certificados e CRLs, para que os utilizadores possam obter a informação que necessitam para a implementação dos seus próprios serviços de segurança;
- Manutenção de arquivos com informação do estado acerca dos seus certificados que já expiraram ou que foram entretanto revogados.

Uma CA pode emitir certificados para utilizadores ou para outras CAs. Quando uma CA emite um certificado está a assegurar que um determinado sujeito possui a chave privada que corresponde à chave pública que está contida no certificado. Quando o sujeito de um certificado for outra CA, a CA emissora assegura que os certificados emitidos pela CA certificadora são igualmente de confiança [PPKI01, UPKCSDC99].

A CA insere a sua identificação em cada certificado ou CRL que gera e assina-os com a sua chave privada. Uma vez estabelecida a confiança numa CA por parte dos utilizadores, estes podem confiar nos certificados que são emitidos por esta. Os utilizadores podem identificar facilmente os certificados emitidos por uma determinada CA através da verificação da identificação desta, contida no certificado. Para assegurar que o certificado é genuíno, é necessário verificar a assinatura contida no certificado usando a chave pública da CA. A identificação da CA é informação pública enquanto que a assinatura da CA é a base da confiança no certificado. Como tal, a principal responsabilidade de uma CA é a de proteger a sua chave privada, mantendo-a secreta.

A informação contida num certificado deve ser igualmente correcta sendo outra das responsabilidades da CA a verificação da informação contida num certificado antes deste ser emitido [UPKICSDC99].

2.3.1.2 Autoridade de Registo

Uma Autoridade de Registo (RA[14]) é utilizada para verificar o conteúdo de um certificado para uma CA. O conteúdo de um certificado deve reflectir a informação apresentada pela entidade que solicita o certificado (Bilhete de Identidade, Carta de Condução, entre outros), assim como informação proporcionada por uma entidade terceira de confiança. A RA agrega esta informação e fornece-a à CA [UPKICSDC99].

Tal como a CA, a RA é composta por *hardware*, *software* e por pessoas que a operam. Cada CA mantém uma lista de RAs acreditadas nas quais confia. Cada RA é identificada perante uma CA pela sua identificação e correspondente chave pública. Através da verificação da assinatura da RA, a CA pode assegurar-se que foi uma RA acreditada que enviou a informação e, como tal, é de confiança.

Existem dois métodos básicos através dos quais uma RA verifica o conteúdo dos certificados. No primeiro, a RA agrega e verifica a informação necessária da entidade requisitante antes do pedido de certificado ser enviado para a CA. A CA confia na informação contida no pedido uma vez que esta foi verificada por uma RA. No segundo método, a CA envia à RA a informação contida num pedido de certificação que recebeu. A RA revê o seu conteúdo e determina se a informação descreve de forma correcta o requisitante do certificado. O primeiro modelo é usado quando o requisitante comparece fisicamente na RA, enquanto que o segundo é usado quando o requisitante não pode ser identificado *a priori* e gera um pedido electrónico de certificado [PPKI01, PKIWTB01].

2.3.1.3 Repositório

As funções básicas de um Repositório consistem na distribuição de certificados e de CRLs. Um Repositório aceita certificados e CRLs de uma ou várias CAs e disponibiliza-os a entidades que deles necessitem para implementar os seus próprios serviços de segurança [UPKICSDC99].

Um Repositório é um sistema que é identificado pelo seu endereço e protocolo de acesso fornecendo certificados e CRLs a pedido, que podem ser baseados na identificação do utilizador, da CA ou noutra informação.

Existem dois modelos básicos de Repositório. No modelo mais comum, o Repositório fornece a informação solicitada sem identificar o solicitador. Existe, também, um modelo alternativo em que o Repositório identifica e autentica cada um dos pedidos efectuados [PPKI01, OSPKIB00].

Uma PKI utiliza um Repositório para armazenar e distribuir certificados e CRLs. Um Repositório é um sistema que é conhecido pelo seu endereço e protocolo de acesso, sendo este último um aspecto bastante crucial uma vez que é usado para aceder ao Repositório.

Os diferentes protocolos de acesso aos Repositórios possuem diversos atributos:

- Localização Transparente;
- Performance e disponibilidade;
- Acesso anónimo versus acesso autenticado;
- Interoperabilidade.

Existem diversos tipos de Repositórios que podem suportar uma PKI, no entanto, a escolha mais tradicional no desempenho desta função recai normalmente na utilização de uma Directoria.

Uma Directoria consiste numa base de dados *on-line* de informação diversa. A informação acerca de uma entidade ou objecto designa-se por "entrada", em que cada uma destas "entradas" está associada a um objecto que descreve os diferentes atributos que uma "entrada" pode conter (Figura 2.17). Para obter informação de uma Directoria, os clientes devem saber para onde devem enviar os pedidos, qual a "entrada" que desejam e qual o atributo dessa "entrada" que necessitam [PPKI01].

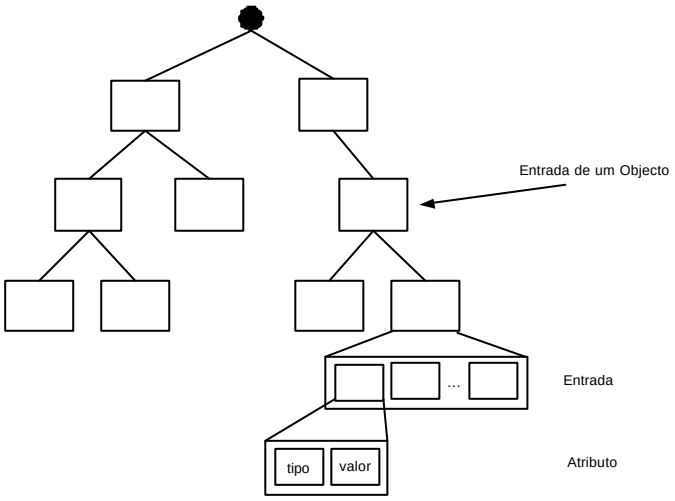


Figura 2.17 Estrutura de uma Directoria

Cada uma destas "entradas" numa directoria é identificada por um nome distinto (DN). Este DN é o mesmo que é utilizado nos campos de um certificado X.509 para identificar o emissor e o detentor do certificado. O cliente poderá solicitar diversos atributos dependendo da informação, no entanto, algumas normas definem um conjunto de atributos padrão [UPKICSDC99]:

[14] *Registration Authority*

- *userCertificate*: o certificado que pertence ao DN do sujeito e à "entrada" na directoria;
- *caCertificate*: o certificado da CA em que o DN do sujeito corresponde à entrada na directoria;
- *certificateRevocationList*: contém CRLs;
- *deltaRevocationList*: contém adições (valores deltas) aos CRLs;
- *crossCertificatePair*: contém um par de certificados CA que são usados para efectuar certificação cruzada;
- *pkiUser*: utilizado para detentores de certificados;
- *pkiCA*: é usado para demarcar entradas de CAs;
- *crlDistributionPoint*: usado para guardar informação sobre revogação de certificados.

Serviço de Directoria X.500

O Serviço de Directoria X.500 é uma base de dados distribuída, com a capacidade para armazenar informação acerca de pessoas e objectos em diversos nós ou servidores distribuídos através de uma rede [PPKI01, PKIEG01]. Os diversos servidores ou nós designam-se por DSA – *Directory Server Agents* e os diversos clientes designam-se por DUA – *Directory User Agent*. Os DSA respondem aos pedidos dos vários DUA (Figura 2.18).

Este serviço de Directoria utiliza dois protocolos base: o *Directory Access Protocol* (DAP) e o *Directory Service Protocol* (DSP). Enquanto que o DAP suporta pedidos de informação de uma DUA para um DSA, o DSP é usado para pedidos entre DSAs.

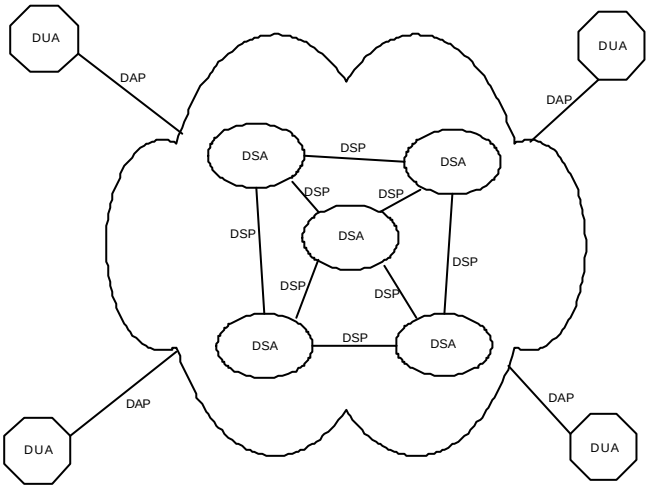


Figura 2.18 Funcionamento e arquitectura do Serviço de Directoria X.500

LDAPv2 – *Lightweight Directory Access Protocol*

Um dos problemas pelo qual o serviço de Directoria X.500 não foi muito bem sucedido deve-se ao facto do protocolo DAP ser demasiado complexo e pesado para a maior parte das aplicações. Com base neste problema foi desenvolvida uma versão menos complexa e pesada do DAP que resultou no protocolo LDAP (*LightWeight Directory Access Protocol*) que foi entretanto normalizado pelo IETF [PPKI01].

Uma das diferenças principais entre o DAP e o LDAP é que no caso do LDAP, as directorias não comunicam entre si. Isto significa que se uma directoria LDAP receber um pedido para uma "entrada" que não faça parte desta, procura numa tabela interna de directorias remotas, retornando uma referência das diversas directorias para a entidade que efectuou o pedido. Depois, é da responsabilidade da entidade solicitadora, efectuar ou não o pedido a outra directoria referenciada pelo serviço.

Serviços de Directoria X.500 com LDAP

Conforme foi referido, o principal ponto fraco do serviço de Directoria X.500 era o protocolo DAP. Com base neste aspecto, a maior parte das implementações de X.500 passaram a suportar em simultâneo DAP e LDAP para que os clientes pudessem optar por usar o protocolo que melhor se adapte às suas necessidades, o que veio acrescentar uma maior flexibilidade ao serviço [PKIETB01, UPKICSDC99].

LDAPv3 com Extensões

O LDAP evoluiu com o trabalho desenvolvido pelo IETF, tendo sido concebida uma nova versão do LDAP (versão 3) contendo algumas extensões, nomeadamente o suporte para efectuar encadeamento de directorias e replicação das mesmas [UPKICSDC99].

2.3.1.4 Arquivo

O Arquivo é responsável pelo armazenamento a longo termo de informação da CA. O arquivo assegura que a informação era boa na altura em que foi recebida e que não foi modificada durante a sua permanência no arquivo. A informação fornecida pela CA ao repositório deve ser suficiente para determinar que o certificado foi emitido efectivamente pela CA tal como é especificado no formato, e que este é temporalmente válido. O arquivo protege a informação através de técnicas e procedimentos apropriados [PPKI01]. No caso de posterior disputa, a informação pode ser usada para verificar que a chave privada associada a um certificado digital foi usada para assinar um determinado documento.

2.3.2 Serviços das PKI

Nesta parte vão ser apresentados quais os serviços nucleares de uma PKI e quais os serviços adicionais proporcionados pelas mesmas.

2.3.2.1 Serviços nucleares de PKI

Considera-se que uma PKI está normalmente associada a três serviços primários: Autenticação, Integridade e Confidencialidade.

Autenticação

A Autenticação permite assegurar que uma entidade é na verdade quem afirma ser. Tem a sua aplicação em dois contextos principais:

- Identificação de entidades: usada para autenticar a entidade envolvida, em isolamento de qualquer outra actividade que a entidade pode desempenhar;

- Identificar a origem dos dados: identifica uma entidade específica como a fonte ou origem de um determinado conjunto de dados [UPKICSDC99].

A identificação de entidades pode ser dividida em duas categorias distintas: identificação da entidade junto do ambiente local e identificação da entidade junto de um dispositivo remoto, entidade ou ambiente.

Enquanto serviço nuclear de uma PKI, a Autenticação faz sentido quando utilizada para autenticação em ambientes remotos, enquanto que autenticação a nível local permite obter acesso à informação da PKI [PKIIMES01].

Um dos benefícios bastante apelativos de um serviço de Autenticação associado a uma PKI é a possibilidade de usar dispositivos *single sign-on* [PKIIMES01].

As PKI oferecem um serviço de Autenticação com um significativo número de vantagens sobre os mecanismos de Autenticação não baseados em PKI. A identificação de entidades é possível com a Autenticação PKI, em que a chave privada da assinatura digital de uma entidade é usada para autenticar essa entidade a outras entidades no ambiente local ou remoto. Pode ser usada igualmente para verificar a autenticidade da origem dos dados. Neste caso, a chave privada da entidade é usada para associar a entidade a um conjunto de dados [PPKI01].

Integridade

A Integridade de dados oferece a garantia da não alteração dos dados, isto é, garante a uma outra entidade que os dados recebidos por esta não foram alterados desde a sua origem [PKIIMES01]. Esta segurança é essencial em qualquer tipo de ambiente de negócio ou de Comércio Electrónico, e é igualmente desejável em muitos outros ambientes. Um nível de Integridade dos dados pode ser obtido através de mecanismos, tais como a utilização de *bits* de paridade e códigos CRC[15]. Tais técnicas, no entanto, são construídas a pensar em detectar erros acidentais ao nível do *bit*. Não são eficazes na determinação da manipulação de dados por entidades terceiras [PKIIMES01].

Para proteger os dados contra este tipo de ataques, são necessárias técnicas criptográficas. Desta forma, devem ser empregues, em comum, algoritmos e chaves entre as entidades que desejem proporcionar Integridade dos dados e aquelas que querem ter a certeza que os mesmos permanecem ou são íntegros. O serviço de Integridade de uma PKI que pode ser extremamente útil para fazer face às necessidades de ambas as entidades, é aquele em que possa ocorrer a selecção dos algoritmos e a concordância de chaves. Para além disso, tais negociações podem ocorrer de uma forma completamente transparente para as entidades envolvidas para que a Integridade possa ser assumida em todas as transacções relacionadas com dados baseados em PKI [UPKICSDC99].

Confidencialidade

A Confidencialidade é a segurança da privacidade dos dados: ninguém pode ler os dados excepto a entidade específica aos quais estes se destinam [PPKI01]. A Confidencialidade é um requisito:

[15] CRC-Code Redundancy Check

- Quando os dados estão armazenados num suporte que pode ser consultado por um indivíduo autorizado;
- Quando os dados são copiados para um dispositivo que pode cair nas mãos de um indivíduo não autorizado;
- Quando os dados são transmitidos em redes desprotegidas [PPKI01].

Dada a sofisticação e a determinação dos adversários dos nossos dias, as técnicas criptográficas que permitem garantir a Confidencialidade devem ser empregues para todos os dados sensíveis. Tal como a Integridade, esta necessita de um conhecimento mútuo de algoritmos e chaves apropriadas entre entidades. O serviço de Confidencialidade de uma PKI é uma ferramenta através da qual esse conhecimento mútuo pode ser obtido de uma forma totalmente transparente para as entidades envolvidas. Serviços de Confidencialidade não baseados em PKI necessitam de interacção explícita entre entidades a algum nível, e portanto estão mais sujeitas a erros ou a incorrecções [PKIIMES01].

2.3.2.2 Serviços adicionais baseados em PKI

Na secção anterior foram identificados os principais serviços nucleares das PKI. A presente secção descreve os serviços de segurança que, de alguma forma, são proporcionados pela utilização das PKI.

Comunicações seguras

Este serviço pode ser definido como a transmissão de dados de um determinado emissor para um receptor utilizando com uma ou várias das seguintes propriedades: Autenticidade, Integridade e Confidencialidade. Este serviço depende dos serviços nucleares das PKI, mas utiliza-os em conjunto com redes e protocolos de comunicação tradicionais para a criação de um serviço estendido proporcionado pela PKI [PKIIMES01]. Exemplos destes serviços são:

- Correio Electrónico Seguro (S/MIME) (ver secção 2.6.1);
- Acesso seguro a servidores de Web (SSL/TLS) (ver secção 2.6.2);
- Redes Privadas Virtuais – VPN (IPSec/IKE) (ver secção 2.6.4).

***Timestamping* Seguro**

O serviço de *Timestamping* seguro envolve a utilização de uma autoridade de confiança de fornecimento de tempo que associa um *timestamp* com um conjunto particular de dados com propriedades de autenticidade e integridade. O que é importante não é o formato temporal (data e hora), mas sim a segurança na relação tempo/dados. Em especial, em algumas aplicações, a necessidade de *Timestamping* não tem explicitamente de representar tempo, bastando uma simples sequência de números que demonstre que determinado documento foi apresentado a uma autoridade antes de outro e depois de outro, pode ser suficiente. No entanto, quaisquer entidades interessadas devem poder verificar que o *timestamp* associado a um documento é autêntico e íntegro [PKIIMES01].

A autoridade de *Timestamping* não é estritamente necessária para este serviço. Uma alternativa é existir uma forma de obter o tempo de uma forma segura no ambiente local de cada entidade; cada uma das entidades pode então associar seguramente um *timestamp* com os seus próprios dados, se necessário. Em termos práticos é particularmente difícil de obter tempo de uma forma segura em todos os ambientes locais. Neste caso, a solução consiste na obtenção de tempo através de autoridades de confiança de fornecimento de *timestamps* de forma segura [PPKI01].

O serviço de *Timestamping* seguro utiliza os serviços nucleares das PKI de Autenticação e Integridade. Em particular, o *timestamp* num documento envolve uma assinatura digital com a combinação de alguma representação de tempo e um *hash* criptográfico do próprio documento.

Para que funcione, as entidades PKI precisam de conhecer e confiar na chave pública da autoridade de emissão do *timestamp* para que a assinatura no *timestamp* possa ser verificada e confiada.

Notariado

O termo Notariado pode ser confundido em alguns ambientes por poder ter significados distintos em diversos contextos. No contexto actual, este serviço refere-se à certificação de dados, isto é, o notário certifica que os dados são válidos ou correctos [PPKI01]. Por exemplo, se os dados a serem certificados forem uma assinatura digital, o notário pode certificar os dados da seguinte forma:

- Certifica que a computação da verificação da assinatura digital com a chave pública certa é matematicamente correcta;
- Certifica que a chave pública é ainda válida e que está associada à entidade que afirma ter assinado o valor;
- Certifica que todos os outros dados necessários no processo de validação estão acessíveis e são de confiança [UPKICSDC99].

O Notário PKI é uma entidade de confiança das outras entidades PKI que permite realizar o serviço de Notariado de uma forma própria e correcta. Certifica a correcção dos dados através de mecanismos de assinatura digital. As restantes entidades PKI necessitam, então, de uma cópia da chave pública de verificação do serviço para que a estrutura de certificação dos dados assinados possa ser verificada e confiada [PPKI01].

O serviço de Notariado baseado em PKI depende de um dos serviços nucleares das PKI que é a Autenticação. Depende igualmente do serviço de *Timestamping* uma vez que o notário precisa de incluir a data e hora em que o serviço de Notariado dos dados foi efectuado na estrutura de certificação dos mesmos.

Não Repúdio

O termo Não-repúdio é usado para o serviço que assegura que as entidades são honestas perante as suas acções [PKIWTB01]. Pode assumir diversas formas:

- Não-repúdio de origem: o utilizador não pode negar ter dado origem a um documento ou mensagem;
- Não-repúdio da recepção: o utilizador não pode negar ter recebido uma mensagem ou documento;
- Não-repúdio da criação: o utilizador não pode negar ter criado uma mensagem ou documento;

- Não repúdio da entrega: o utilizador não pode negar ter entregue uma mensagem ou documento;
- Não repúdio da aprovação: o utilizador não pode negar ter aprovado uma mensagem ou documento.

A ideia base é a de que um utilizador está criptograficamente ligado a uma acção específica de tal forma que a subsequente negação de tal acção constitui um acto malicioso [PKIMES01, TRPKI00].

O Não-repúdio é um serviço baseado em PKI, que depende da existência de outros serviços baseados em PKI para funcionar devidamente. Necessita do serviço de *Timestamping* seguro para fornecer provas que um determinado evento ocorreu num determinado momento. Necessita igualmente do serviço de Notariado que é usado para garantir e incluir provas nas estruturas de certificação próprias para armazenamento. Estes serviços dependem ainda dos serviços nucleares PKI: Autenticação, Integridade e Confidencialidade.

Gestão de Privilégios

A Gestão de Privilégios é um termo genérico que é usado para representar um conjunto de actividades, tais como autorização, controlo de acessos, gestão de direitos, gestão de permissões ou gestão de capacidades, entre muitas outras. Este serviço especifica o que a uma entidade é permitido fazer ou visualizar num determinado ambiente [UPKICSDC99].

Definem-se políticas ou regras para indivíduos, grupos particulares ou entidades. Estas políticas especificam o que é permitido, ou não, fazer por essas entidades ou grupos. A Gestão de Privilégios é a criação e aplicação destas políticas com o propósito de permitir a execução normal de acções nas organizações com o nível desejado de segurança [UPKICSDC99].

Neste aspecto da Gestão de Privilégios é importante distinguir entre os conceitos de autenticação e de autorização. Enquanto que a autenticação está preocupada com quem é a entidade a autorização está preocupada com o que é que uma entidade é permitida fazer ou ver. Tanto a Autenticação como a Autorização podem e devem funcionar em simultâneo em muitas circunstâncias. A autenticação sem autorização é útil em algumas circunstâncias e por outro lado a autorização sem autenticação não possui muito valor.

No mundo electrónico, devem existir autoridades de autorização que associam privilégios específicos com identidades, grupos ou papéis específicos num determinado ambiente, utilizando técnicas criptográficas, embora a sua presença possa ser explícita ou implícita [PPKI01, UPKICSDC99].

A noção de privilégio pressupõe igualmente uma outra noção de delegação. Se uma entidade possui um determinado privilégio então pode passar esse mesmo privilégio para outra entidade. Esta delegação pode ocorrer de duas formas: através de delegação cega, quando uma entidade deseja delegar algum privilégio noutra em que a autoridade que verifica a autorização desta não consegue determinar que esta delegação ocorreu; através de delegação não cega, em que é óbvio para a entidade que verifica a autorização que uma entidade passou um determinado privilégio para outra durante um determinado período de tempo [PKIIMES01].

2.3.3 Mecanismos das PKI

Nesta parte encontram-se identificados e descritos alguns dos mecanismos das PKI.

2.3.3.1 Certificação cruzada

O mecanismo de certificação cruzada é bastante útil permitindo efectuar a ligação entre duas CAs que anteriormente não estavam relacionadas, para que possa existir confiança mútua entre as diversas comunidades de entidades e utilizadores que certificaram. Este mecanismo de certificação é idêntico ao de certificação normal, no entanto, a diferença principal reside no facto que a entidade a ser certificada é ela própria uma CA.

Esta certificação cruzada pode ocorrer em dois sentidos, isto é uma CA1 pode certificar de forma cruzada uma CA2 sem que a CA2 tenha certificado de forma cruzada a CA1 (unilateral) ou ambas se podem certificar de forma cruzada uma à outra (mútua).

Este mecanismo de certificação cruzada pode ser utilizado para aumentar a confiança entre as diferentes comunidades de entidades, permitindo que diferentes CAs possam confiar nas credenciais que cada uma destas emite. Isto vai permitir que PKI distintas possam facilmente interoperar entre si em termos de confiança [UPKICSDC99].

2.3.3.2 Caminhos de Certificação

Um caminho de certificação é um elemento fundamental das PKI. É um método que significa uma cadeia de certificados em que o emissor do primeiro certificado é designada como base de confiança e a entidade certificada no último certificado é a entidade certificada. Uma aplicação baseada em PKI deve poder construir e validar todo o caminho de certificação antes de poder confiar na chave pública contida no certificado [PPKI01, OSPKIB00].

As aplicações de PKI devem verificar um certificado antes de usar a chave pública contida no mesmo, para poderem efectuar operações criptográficas. A aplicação não pode confiar na chave pública excepto se existir um caminho de certificação válido. A aplicação é inicializada para reconhecer caminhos que comecem com uma ou mais CAs. Estas CAs são também designadas por “pontos de confiança”.

Existem dois processos principais no processamento dos caminhos de certificação (Figura 2.19):

- Construção do Caminho, que envolve a agregação de todos os certificados necessários para formar o caminho completo;
- Validação do Caminho, que envolve examinar cada um dos certificados no caminho, determinando se a chave que contém pode ser de confiança ou não.

Um caminho de certificação é portanto uma sequência de certificados. Para que esta sequência de certificados seja válida devem ser satisfeitos os seguintes requisitos:

- O emissor do primeiro certificado deve ser um “ponto de confiança”;
- O último certificado deve ter sido emitido para a entidade final e conter a sua correspondente chave pública;

- Os nomes distintos do emissor e da entidade certificada formam uma cadeia. Para todos os certificados na sequência, à excepção do primeiro e do último, o nome do emissor deve corresponder ao nome do sujeito no certificado anterior e o nome do sujeito corresponde ao nome do emissor no certificado subsequente;
- Todos os certificados se encontram dentro do período de validade [PPKI01, OSPKIB00].

O processo formal para efectuar a verificação dos caminhos de certificação pode ser reduzido aos seguintes quatro passos [PPKI01]:

- Inicialização;
- Verificação básica do Certificado;
- Preparação para o próximo certificado na sequência;
- Processamento final e Resultado.

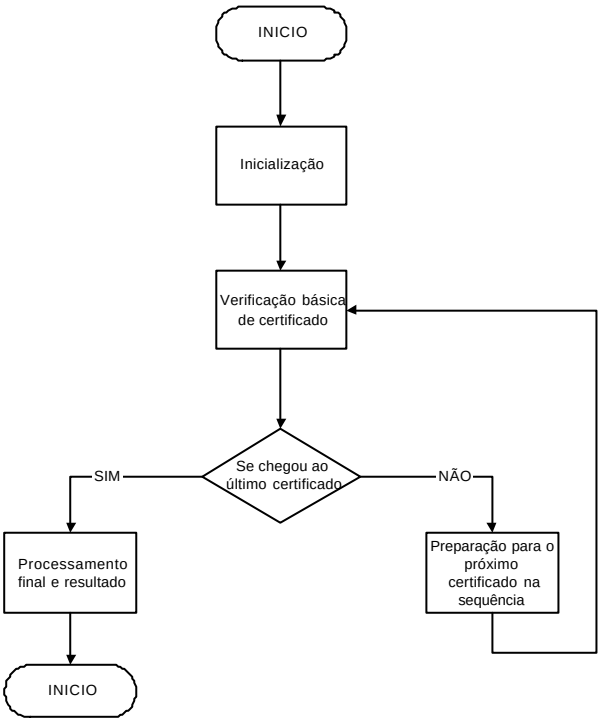


Figura 2.19 Processamento de cadeias de Certificação

2.3.3.3 Gestão de Chaves e de Certificados

O conceito de chave pública pressupõe a existência de um par de chaves: uma pública e outra privada. Enquanto que uma chave pública é na maior parte das vezes distribuída sob a forma de um certificado, a chave privada é mantida numa estrutura de dados separada e sempre protegida (tanto em trânsito, como em utilização, ou quando armazenada). O termo gestão do ciclo de vida das chaves e/ou certificados denota as funções de gestão do ciclo de vida associados com a criação, emissão, e subsequente cancelamento dos pares de chaves e os seus certificados associados. A gestão do ciclo de vida das chaves e certificados fazem parte das funções de qualquer PKI [UPKICSDC99, OSPKIB00].

2.3.3.4 Revogação de certificados

Os certificados são principalmente utilizados para ligar uma entidade com um determinado atributo, por exemplo uma entidade com a correspondente chave pública. Normalmente, esta ligação é válida ao longo da vida útil do certificado, no entanto, por outras circunstâncias, este pode deixar de ser válido antes de terminar a sua vida útil. Deve então existir um mecanismo que permita avisar as entidades que vão verificar os certificados que estes já não são válidos ou que se encontram revogados. Esta revogação é de extrema importância e deve ser usada da forma mais eficiente possível, pois durante o período que decorre entre um certificado ser revogado e todas as entidades serem avisadas desta revogação, podem ser cometidas utilizações fraudulentas do certificado entretanto já revogado [PKIWTB01, PPKI01, TRPKI00].

Existem dois mecanismos fundamentais para a implementação da revogação de certificados (mais detalhes sobre cada um destes mecanismos poderá ser encontrada no Anexo F, Tabela F.7):

- Mecanismos de Publicação Periódica, cujos mais utilizados são os seguintes [PPKI01]:
  - CRLs Completas (CRLs);
  - *Authority Revocation Lists* (ARLs);
  - Pontos de distribuição de CRLs (DpCRLs);
  - CRLs Delta (dCRLs);
  - CRLs indirectas (iCRLs);
  - Pontos melhorados de distribuição de CRLs (DEpCRLs);
  - Árvores de Revogação de Certificados (CRTs).
- Mecanismos de Pesquisa *On-line*:
  - *On-line Certificate Status Protocol* (OCSP).

Sempre que um certificado precise de ser revogado a CA coloca o identificador do certificado em questão numa lista designada por CRL.

A norma X.509 define uma estrutura de informação própria (Figura 2.20) para esta CRL, que é assinada pelo emissor do CRL e codificada em ASN.1 DER [UPKICSDC99, PKIIMES01].

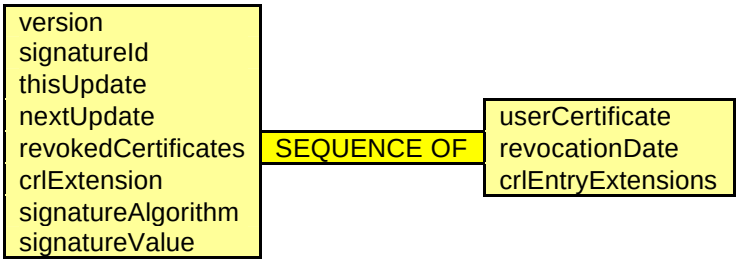


Figura 2.20 Formato X.509 para uma CRL

- *tbsCertList*: o conteúdo do CRL;

- *signatureAlgorithm*: o identificador do algoritmo de assinatura digital usado para assinar a CRL;
- *signatureValue*: o valor da assinatura digital.
- *version*: indica a versão do formato da CRL;
- *signature*: contém o identificador do algoritmo usado pelo emissor do CRL para assinar a lista de certificados do CRL;
- *issuer*: contém o DN do emissor do CRL;
- *thisUpdate*: a data de emissão do CRL;
- *nextUpdate*: a data de emissão do próximo CRL;
- *revokedCertificates*: uma lista dos certificados que foram revogados
- *userCertificate*: especifica o número de série do certificado a ser revogado;
- *revocationDate*: especifica a data em que a revogação do certificado ocorreu;
- *crlEntryExtensions*: extensão específica deste certificado na CRL;
- *crlExtensions*: extensão específica do CRL.

2.4 Arquitecturas e Modelos de Confiança das PKI

Esta parte do capítulo identifica as principais arquitecturas de PKI, assim como os principais modelos de confiança que podem ser estabelecidos através da utilização das mesmas.

2.4.1 Arquitecturas das PKI

São diversas as arquitecturas de PKI existentes. No entanto, de entre todas essas arquitecturas destacam-se as que de seguida se apresentam com maior detalhe.

2.4.1.1 A Arquitectura PKIX

O grupo de trabalho PKIX foi estabelecido pelo IETF, no final de 1995, com o objectivo de desenvolver um conjunto de normas para a Internet necessárias para suportar uma PKI baseada em X.509 [UPKICSDC99, OCSX509CA98].

A norma X.509 define os campos, o formato dos certificados e os procedimentos para a distribuição de chaves públicas. Como o X.509 é uma norma bastante abrangente que deve contemplar muitos campos de aplicação, permite diversas variações nos conteúdos dos certificados e suporta múltiplos modelos operacionais. Subconjuntos das funcionalidades do X.509 podem ser definidas para comunidades particulares e para campos de interesse distintos [OCSX509CA98].

No entanto, o grau de abrangência do trabalho do PKIX estendeu-se para além do seu objectivo inicial e não apenas introduz modificações nas normas iniciais do ITU-T assim como produz igualmente um conjunto de normas próprias.

O PKIX identifica as funções principais de uma PKI como sendo [UPKICSDC99]:

- Registo;
- Inicialização;
- Certificação;
- Recuperação de Pares de Chaves;
- Geração de Chaves;
- Actualização de Chaves;
- Certificação cruzada;
- Revogação;
- Distribuição/Publicação dos Certificados e de Revogação.

O PKIX desenvolveu vários documentos que descrevem as cinco grandes áreas de suporte ao seu modelo de arquitectura. Estas áreas incluem:

- Certificados X.509v3 e CRLsv2;
- Protocolos operacionais;
- Protocolos de Gestão;
- Políticas de Gestão;
- Serviços de certificação de dados e de *Timestamping*.

Estas divisões permitem o refinamento do X.509 de várias formas, uma vez que existe uma definição de perfis que permitem a subdivisão do X.509 para que inclua extensões específicas bastante úteis para a utilização na comunidade Internet.

Os principais componentes de uma arquitectura PKIX incluem [PPKI01] (Figura 2.21):

- Clientes:
    - O utilizador de um certificado de uma PKI, também identificado como entidade final;
    - O utilizador final ou sistema é o sujeito de um certificado PKI.
- Autoridade de Certificação (CA):
    - Emite e revoga certificados PKI.
- Autoridade de Registo (RA):
    - Garante que a associação entre as chaves públicas e a identidade dos detentores dos certificados é de confiança.
- Repositório:

- Um sistema (distribuído ou não) que armazena certificados e CRLs;
- Oferece um mecanismo de distribuição para certificados e CRLs a entidades finais.

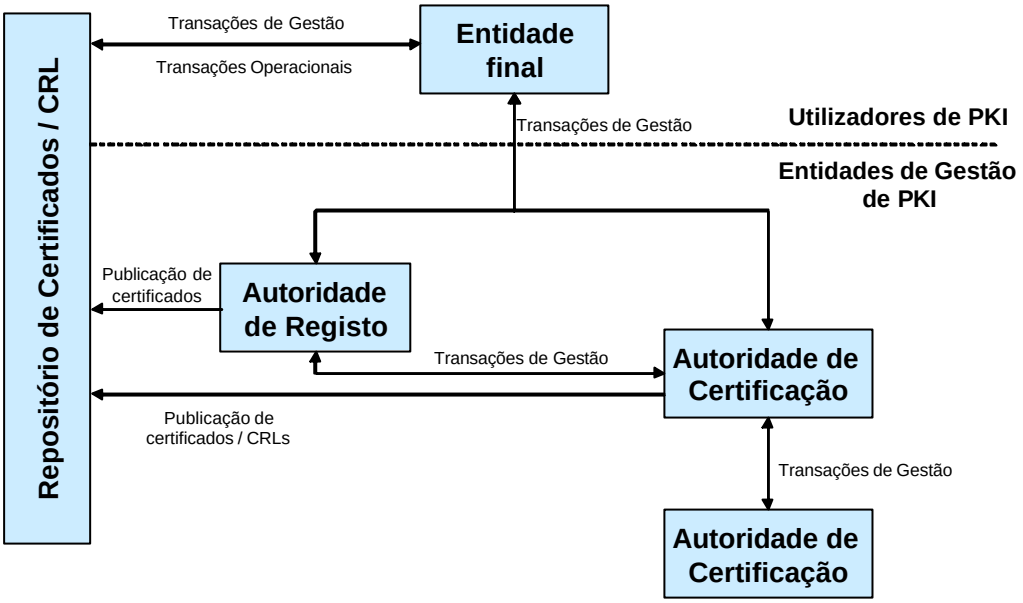


Figura 2.21 A arquitectura PKIX

As transacções operacionais são as trocas de mensagens que estão incluídas nos documentos dos protocolos operacionais e que oferecem a camada de transporte para certificados, CRLs e outra informação de gestão dos mesmos. As transacções de gestão são trocas de mensagens descritas nos documentos dos protocolos de gestão que oferecem os serviços de mensagens para suportar as transacções de gestão. A publicação é utilizada para distribuir certificados e CRLs para repositórios públicos [PPKI01, PKIIMES01].

2.4.1.2 A Arquitectura APKI do OpenGroup

O *OpenGroup* definiu num documento designado por APKI – *Architecture for Public Key Infrastructure*, a sua própria arquitectura de PKI, baseado igualmente em X.509, listando quais as funcionalidades específicas que deveriam ser proporcionadas por uma PKI [APKI99].

Os componentes da arquitectura de uma PKI estão agrupados em diversas categorias funcionais (Figura 2.22) genéricas:

- Serviços que Permitem a Segurança do Sistema

  Providenciam a funcionalidade que permite que a identidade de um utilizador ou outro principal possa ser estabelecida e associada com as suas acções no sistema.

- Primitivas e Serviços Criptográficos

  Providenciam as funções criptográficas nas quais é baseada a segurança da chave pública.

- Serviços de Chaves de Longa Duração

Permite que utilizadores ou outras entidades possam gerir as suas chaves e certificados de longo termo e verificar a validade dos certificados de outras entidades.

- Serviços de Segurança dos Protocolos

  Providenciam funcionalidades de segurança (autenticação da origem dos dados, integridade dos dados, protecção de dados, não repúdio) adequadas para a implementação de aplicações de segurança, tais como protocolos de segurança.

- Protocolos de Segurança

  Providenciam comunicações seguras entre aplicações que não possuam ou possuam poucas funcionalidades de segurança integradas.

- Serviços da Política de Segurança

  Providenciam informação relativa à política que deve ser conduzida em protocolos seguros para permitir o controlo de acessos.

- Serviços de Suporte

  Providenciam a funcionalidade que é requerida para a operação segura mas que não está directamente envolvida na execução da política de segurança [APKI99].

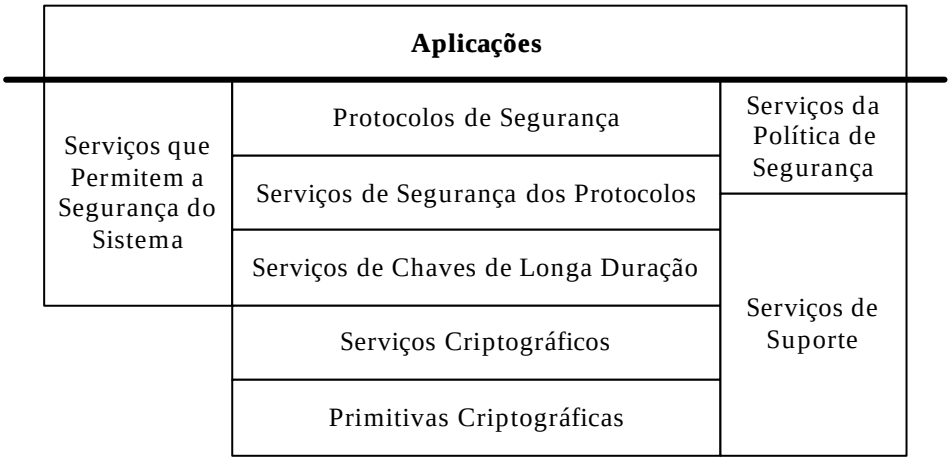


Figura 2.22 A Arquitectura PKI

Uma descrição mais detalhada e exaustiva poderá ser encontrada no Anexo F, Tabela F.8.

2.4.1.3 A Arquitectura SPKI – *Simple Public Key Infrastructure*

O grupo de trabalho IETF SPKI foi criado em 1996 como alternativa ao esforço do PKIX [SPKICT98]. A necessidade de ter um formato de certificados mais flexível e simples que o X.509 foi uma das grandes motivações do SPKI. Portanto, uma das premissas fundamentais deste grupo é a de que o X.509 é um formato de certificado demasiado complexo que associa uma identidade a um par de chaves. O SPKI argumenta que o conceito de um identificador de identidade globalmente único não é possível, e que a

chave pública é a única identidade de relevância. No entanto, sempre que se verifique ser necessário ou útil a associação de um nome ou outra informação de identificação esta pode ser realizada [SPKICT98].

O sofisticado formato dos certificados SPKI torna possível expressar de uma forma geral o que uma chave é capaz de fazer. Ao contrário do enfoque inicial do X.509 e do PKIX, o SPKI suporta tanto a autenticação, como a autorização.

Apesar do SPKI possuir algumas ideias interessantes, não conseguiu ganhar um número suficiente de apoiantes tanto a nível empresarial, como governamental, tal como sucedeu com o X.509, embora seja ainda alvo de desenvolvimento e de discussão por parte da comunidade científica [UPKICSDC99].

SDSI – *Simple Distributed Security Infrastructure*

O SDSI representa um esforço independente para desenvolver uma PKI mais simples. O SDSI é semelhante ao SPKI no que diz respeito à chave pública ser o identificador principal, em conjunto com outros dados associado a esta. A funcionalidade principal acrescentada pelo SDSI foi a noção de *namespaces* (definidos relativamente a uma chave particular) [SPKISDSIWT00].

Um nome SDSI é definido como sendo uma sequência de tamanho autónomo, consistindo numa chave pública e por zero ou mais identificadores.

SPKI/SDSI

Os dois grupos de trabalho juntaram-se num único esforço de colaboração mútua designado por SPKI/SDSI. Este esforço usou partes do SPKI e do SDSI e eliminou algumas funcionalidades menos populares. O SPKI/SDSI combina os nomes SDSI com a delegação de autoridade do SPKI, embora continue a não obter grande relevância em termos de utilização [SPKISDSIWT00].

2.4.2 Modelos de Confiança das PKI

Os modelos de confiança baseados em PKI são importantes uma vez que permitem responder a questões como: quais os certificados digitais que uma entidade pode confiar? Como é que a confiança pode ser estabelecida e de que forma é que a confiança pode ser controlada num determinado ambiente [UPKICSDC99, PKIIMES01]?

Uma boa definição de confiança pode ser a seguinte: “uma entidade A confia numa entidade B quando A assume que B irá ter um comportamento igual ao que A espera” [UPKICSDC99]. A confiança é assim construída na base de suposições, expectativas e comportamentos, não podendo ser medida quantitativamente, pelo que existe sempre um risco associado com a mesma. Devido a esse risco, nem sempre é possível estabelecer uma relação de confiança de forma automática.

De seguida apresentam-se quatro dos tipos de modelos de confiança mais utilizados pelas PKI: Hierarquia de Autoridades de Certificação, Arquitectura Distribuída de Confiança, Modelo em Rede e Confiança Centrada no Utilizador [UPKICSDC99, PKIIMES01].

2.4.2.1 Hierarquia de Autoridades de Certificação

Este tipo de modelo pode ser representado como uma árvore invertida (raiz no topo e folhas na parte de baixo). A raiz desta árvore corresponde à Autoridade de Certificação (CA) de topo para o domínio inteiro da PKI (Figura 2.23). Abaixo desta CA existem CAs intermédias. As folhas desta árvore correspondem normalmente aos utilizadores finais[16] [PKIIMES01].

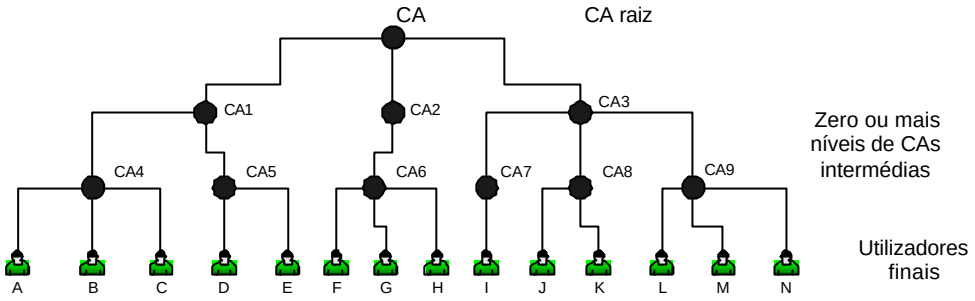


Figura 2.23 Hierarquia de Autoridades de Certificação

Neste modelo, todas as entidades na hierarquia confiam numa única CA de topo. A hierarquia é estabelecida da seguinte forma:

- A CA de topo certifica zero ou mais CAs imediatamente abaixo dela;
- Cada uma destas CAs certifica zero ou mais CAs imediatamente abaixo delas;
- No final da hierarquia as CAs certificam utilizadores finais.

Como é que os utilizadores finais confiam uns nos outros? Por exemplo, como é que um utilizador 'A' confia no utilizador 'E' e vice-versa? O utilizador 'A' possui um certificado com o seguinte caminho de certificação (CA_4, CA_1, CA) e 'E' com (CA_5, CA_1, CA). Como no caminho de certificação de ambos existe uma CA em comum (CA_1) então ambos podem estabelecer confiança entre si. Em último caso esta procura poderia ascender até à CA de topo desta hierarquia.

Este modelo de confiança é o mais adequado para entidades com uma dimensão fixa (por exemplo uma empresa) e menos adequado para ambientes mais vastos (por exemplo a Internet), uma vez que obriga à existência de um único ponto centralizado. Um exemplo da aplicação deste modelo de confiança pode ocorrer por exemplo numa organização que esteja organizada por departamentos e secções. A organização possui uma CA de topo que irá certificar cada uma das diversas CAs departamentais. Por sua vez, cada CA departamental pode ainda certificar várias CAs de secções da empresa, que por sua vez emitem certificados para os seus diversos colaboradores e aplicações. É assim possível estabelecer relações de confiança electrónica entre colaboradores de secções e departamentos diferentes da mesma organização, sem que estes tenham que se conhecer fisicamente.

[16] Por utilizadores finais, não se entendam apenas indivíduos (pessoas) como também entidades, *software* ou outros.

2.4.2.2 Arquitectura Distribuída de Confiança

Ao contrário do anterior modelo de confiança, em que todas as entidades dependiam de uma única CA de topo, neste modelo a confiança é partilhada e distribuída por várias CAs [UPKICSDC99].

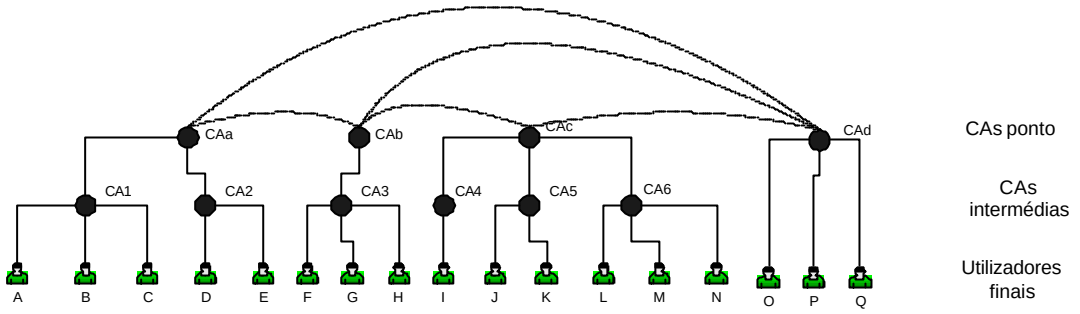


Figura 2.24 Hierarquia Distribuída de Confiança

O processo de interligação entre as diversas CAs ponto designa-se por certificação cruzada, em que ambas certificam a chave pública de cada uma delas. A certificação cruzada é um mecanismo extremamente útil para relacionar CAs que previamente não se encontravam de todo relacionadas (Figura 2.24).

Neste modelo podem ocorrer dois tipos distintos de certificação cruzada [UPKICSDC99] (ver secção 2.3.3.1). No primeiro tipo, pode acontecer que todos os certificados das CAs de topo são cruzados uns com os outros, dando origem a uma malha de certificações cruzadas (todos estão certificados de forma cruzada com todos). No segundo tipo cada CA de raiz efectua uma certificação cruzada com uma única CA central cuja função é a de facilitar a interligação entre as diversas CAs. Esta CA central pode ser interna ou externa às organizações e actua como uma "ponte" entre os sistemas PKI das diferentes organizações. A diferença entre esta configuração e a anterior é que cada CA apenas precisa de efectuar uma certificação cruzada com esta CA central (é uma aproximação ao modelo apresentado anteriormente).

Este modelo de confiança é particularmente adequado para o estabelecimento de relações electrónicas entre parceiros de negócio de diferentes organizações. Cada uma das organizações poderá ter um modelo de PKI organizado em hierarquia a funcionar internamente, mas quando ambas as organizações resolvem estabelecer relações de segurança electrónica entre si (por exemplo clientes e fornecedores) torna-se necessário alterar o modelo de confiança. Assim, o modelo de confiança mais adequado para este caso é o de Hierarquia Distribuída de Confiança, pois através do cruzamento dos certificados das CAs raiz de cada uma das organizações será possível que utilizadores de uma organização possam confiar em outros utilizadores da outra organização, sem o prévio contacto físico entre ambos.

2.4.2.3 Modelo em Rede

O modelo em rede deve o seu nome à *World Wide Web* e está dependente dos tradicionais *browser* de *Web* (Netscape Navigator e Microsoft Internet Explorer, por exemplo) [PKIIMES01].

Neste tipo particular de modelo, um determinado número de chaves públicas pertencentes a CAs estão pré-instaladas nos *browsers* (Figura 2.25). Estas chaves definem o conjunto de CAs em que a utilização do

browser inicialmente confia para funcionar como raiz para verificação dos certificados [UPKICSDC99, WSCRTS97].

Embora este conjunto de chaves raiz possa ser alterado pelo utilizador, é reconhecido que poucos utilizadores dos *browsers* são suficientemente evoluídos para modificar estes aspectos de segurança.

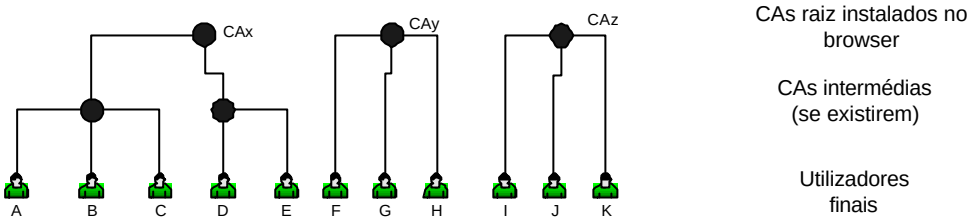


Figura 2.25 Modelo em Rede

O modelo em rede apresenta algumas vantagens em termos de conveniência e simplicidade. No entanto, existe um largo número de implicações de segurança com este modelo que devem ser tidas em consideração quando são tomadas decisões de implementação num determinado ambiente [UPKICSDC99]. Por exemplo, uma vez que os utilizadores de *browsers* confiam automaticamente num conjunto de chaves públicas pré-instaladas, a segurança poderá estar comprometida se uma destas CAs raiz for igualmente comprometida, o que poderá levar o utilizador a confiar nela como se esta fosse de confiança.

Outro dos potenciais problemas de segurança deste modelo é o de que não existe nenhuma forma fácil de revogar qualquer das chaves raiz embebidas no *browser*. Caso se descobrisse que uma das CAs era maliciosa ou que a correspondente chave privada havia sido comprometida era quase impossível descontinuar a utilização dessa chave nos vários milhões de cópias dos *browsers* de *Web* espalhados pelo mundo.

Este é o modelo de confiança que está implementado no protocolo SSL/TLS[17] (ver secção 2.6.2) que é actualmente o mais utilizado na *World Wide Web* para segurar transacções electrónicas realizadas entre os *browsers* de *Web* e os servidores de *Web*. Este modelo permite que um utilizador de um *browser* de *Web* possa confiar num determinado servidor de *Web,* porque este possui um certificado instalado que foi emitido por uma CA cuja chave raiz está instalada no *browser* de *Web* do utilizador. Na prática, este é o actual mecanismo que faz com que eventuais compradores possam confiar em lojas electrónicas e na segurança da transmissão dos seus dados pessoais que podem incluir dados de pagamento.

Este modelo tem bastante sucesso pois a sua utilização por parte do utilizador é totalmente transparente para este, e mesmo para quem deseja implementar lojas electrónicas os requisitos técnicos não são demasiado complexos.

Este tipo de modelo de confiança é mais utilizado para o Comércio Electrónico do tipo *Business-to-Consumer* (B2C), embora possam existir algumas variantes a este modelo.

[17] Secure Sockets Layer/Transport Layer Security

2.4.2.4 Confiança Centrada no Utilizador

Neste modelo de confiança, cada utilizador é directamente e totalmente responsável por decidir quais são os certificados em que confia. Esta decisão pode ser influenciada por um número de factores, embora o conjunto inicial de chaves de confiança possam incluir as de amigos, familiares ou colegas que o utilizador conhece pessoalmente [UPKICSDC99, PKIIMES01].

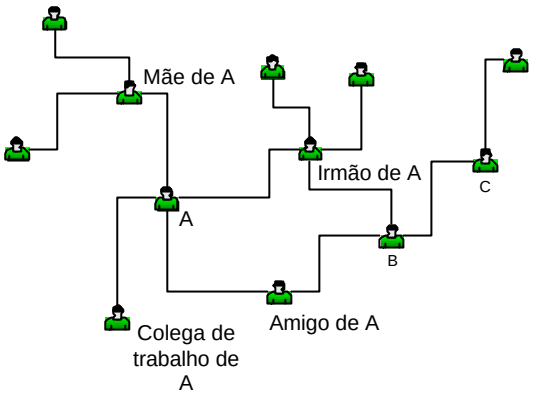


Figura 2.26 Modelo de Confiança Centrada no Utilizador

Por causa da dependência das acções e decisões dos utilizadores este modelo de confiança pode funcionar bem em comunidades científicas, mas é pouco realista para a comunidade em geral. Mais, este modelo é geralmente inapropriado para ambientes empresariais, financeiros ou governamentais uma vez que estes desejam exercer algum controlo sobre a confiança dos utilizadores. Estas políticas de confiança organizacional não podem ser implementadas neste modelo de confiança (Figura 2.26).

O PGP ou *Pretty Good Privacy* [NAICPGP00] (ver secção 2.2.6.3) é uma ferramenta que se baseia neste modelo de confiança, e que foi criada por *Phil Zimmermann* para protecção dos dados pessoais.

Este modelo é adequado para ambientes em que os utilizadores já tenham estabelecido outro tipo de relação de confiança à priori, uma vez que são os utilizadores que decidem em quem confiam (numa organização pequena em que todos os utilizadores se conhecem pessoalmente). Apesar de ser igualmente fácil de estabelecer e de utilizar (embora menos transparente que o modelo anterior), não é muito adequado para utilização no Comércio e Negócio Electrónico.

A grande vantagem deste modelo face ao anterior reside no facto de que o mecanismo de estabelecimento de confiança não depender de entidades externas (como acontece no caso dos *browsers*), mas ser deixado ao cuidado do próprio utilizador.

2.5 Políticas e Procedimentos em PKI

Quando se faz referência a uma PKI muitas vezes apenas se têm em consideração os aspectos técnicos que na verdade são por vezes insuficientes quando utilizados por si só. Estes aspectos ou mecanismos são utilizados normalmente em conjunto com uma série de procedimentos que permitem implementar uma determinada política de segurança. Existem dois tipos de documentos que descrevem os procedimentos e políticas associadas a uma PKI: um deles designa-se por Políticas de Certificação (*Certificate Policy* (CP)) e

outro por Declaração de Práticas de Certificação (*Certificate Practices Statement* (CPS)). Apesar destes documentos partilharem um formato comum as suas audiências e os seus objectivos são diferentes [DPCC97, UPKICSDC99].

A CP é um documento de alto-nível que descreve a política de segurança para a emissão de certificados e a manutenção da informação de estado dos mesmos. A política de segurança descreve a operação da CA assim como a responsabilidade dos utilizadores na solicitação e utilização de certificados e chaves. A CP assegura igualmente como a política será implementada [PPKI01].

A CPS é um documento extremamente detalhado que descreve como uma CA deve implementar uma CP específica. A CPS identifica a CP e especifica os mecanismos e os procedimentos que são utilizados para obter a política de segurança. A CPS assegura que determinados produtos específicos serão utilizados em conjunto com procedimentos específicos [PPKI01].

Tanto a CP como a CPS obedecem a um formato especificado no documento RFC2527 [RFC2527] que estabelece um índice com cerca de oito tópicos principais:

- Introdução;
- Considerações Gerais;
- Identificação e Autenticação;
- Requisitos Operacionais;
- Controlo da Segurança Pessoal, Física e Procedimental;
- Controlos de Segurança Técnica;
- Perfis de certificados e de CRLs;
- Especificações administrativas.

O desenvolvimento de uma política de certificação para uma organização requer a integração necessária de considerações de ordem legal, técnica e de negócio. A integração bem sucedida destas visões dispersas é inerentemente um exercício político, em que a aceitação de uma CP requer o envolvimento de elementos-chave da organização [PKIIMES01].

Para a implementação de uma CP são necessários os seguintes passos:

1. Compreensão dos objectivos da organização e dos seus requisitos que criaram a necessidade por uma PKI, assim como a revisão do conceito de operação para a organização e a arquitectura do sistema proposto.
2. Obtenção de uma cópia do RFC2527 [RFC2527] e de algumas políticas exemplo que partilham os objectivos da organização.
3. Elaboração de uma CP que faça sentido na organização.
4. Decisão de operar uma CA própria ou recorrer aos serviços de uma CA externa.

5. Elaboração de documentação, ou seja, desenvolvimento de uma CPS. Se se optar por operar uma CA própria, a CPS identifica os sítios físicos que irão ser utilizados, mapeando os papéis na CP para os papéis e procedimentos suportados pelo produto PKI e controlos físicos. Se se optar por usar serviços de uma CA externa, a CA fornecedora do serviço deverá possuir uma CPS [RFC2527].

2.6 Aplicações baseadas em PKI

Hoje em dia, existem diversas aplicações que são baseadas em PKI sendo utilizadas como ferramentas de segurança de grande divulgação [UPKICSDC99]. Algumas destas aplicações são:

- S/MIME: proporciona segurança para o correio electrónico baseado na Internet. Pode ser utilizado para assinar digitalmente e encriptar mensagens de correio electrónico;
- SSL/TLS: proporciona autenticação e encriptação num canal de comunicação. SSL/TLS é usado mais para protecção de conteúdo na Web mas pode ter outras aplicações;
- SET: proporciona segurança nas transacções realizadas na Web, com especial importância para os cartões de crédito;
- IPSec: proporciona autenticação e encriptação para pacotes individuais (datagramas).

2.6.1 S/MIME – *Secure/Multipurpose Internet Mail Extensions*

O S/MIME proporciona a utilização do correio electrónico em segurança. O correio electrónico é dos serviços mais utilizados na Internet, sob as mais variadas formas. É um serviço com bastante importância e, como tal, várias têm sido as tentativas para normalizar a segurança do mesmo: PEM, PGP, OpenPGP e S/MIME [PPKI01]. De entre todas estas ferramentas de segurança de correio electrónico que dependem de uma PKI, o S/MIME é a que se encontra mais implementada e divulgada [PPKI01].

O S/MIME define dois cabeçalhos MIME: um para assinaturas digitais e outro para encriptação sendo ambos baseados na norma PKCS#7 (consultar Anexo F, Tabela F.6).

Em termos de funcionalidade geral, o S/MIME é muito semelhante ao PGP: ambos oferecem a possibilidade de assinar e/ou encriptar mensagens. As funcionalidades básicas do S/MIME incluem:

- Criação de envelopes de dados;
- Assinatura digital de dados;
- Dados assinados digitalmente e transmitidos em claro;
- Dados assinados digitalmente e colocados em envelope [NSEAS00, RSALFAQ00].

O S/MIME utiliza certificados de chave pública X.509v3. A hierarquia de confiança adoptada pelo S/MIME é híbrida e varia entre o modelo hierárquico X.509 e a teia de confiança do PGP. Tal como no modelo PGP, os utilizadores configuram as aplicações cliente com uma lista de chaves de confiança e de CRLs. Assim, a responsabilidade é local para a manutenção dos certificados necessários para verificação das assinaturas

digitais e encriptação de mensagens. Por outro lado, os certificados são assinados por autoridades de certificação (endereço de correio electrónico ligado com chave pública) [NSEAS00, PPKI01].

Um utilizador S/MIME possui várias funções de gestão de chaves, nomeadamente:

- Geração de chaves;
- Registo numa Autoridade de Certificação;
- Armazenamento e Pesquisa de Certificados.

2.6.2 SSL/TLS – *Secure Sockets Layer/Transport Layer Security*

O SSL/TLS proporciona segurança para transações entre aplicações no canal de comunicação, mais concretamente entre o *browser* de Web e um servidor de Web (embora possa igualmente ser utilizado noutras aplicações). Depois do correio electrónico, a Web é dos serviços mais usados que são proporcionados pela Internet [SSLTLS99].

Inicialmente, quando a *Netscape Communications* publicou a norma SSL, na tentativa de ganhar maior aceitação disponibilizou as especificações ao IETF. Como resultado, foram introduzidos vários melhoramentos pelo IETF que culminaram no TLS, uma versão melhorada do SSL [SSLTLS99, NSEAS00].

O objectivo do SSL e do TLS é o de proporcionar autenticação, integridade e confidencialidade entre duas aplicações em comunicação. Os protocolos são compostos por dois níveis: o nível de mensagens (protocolo *Handshake*) e o nível de comunicação (protocolo *Record*). O protocolo *Handshake* autentica o cliente e o servidor, negoceia o algoritmo de encriptação e estabelece as chaves criptográficas (Figura 2.27). O protocolo *Record* encapsula e protege os protocolos dos níveis superiores (Figura 2.27) [SSLTLS99]. Mais detalhes sobres estes dois protocolos podem ser consultados no Anexo F, Tabela F.9 e F.10 respectivamente.

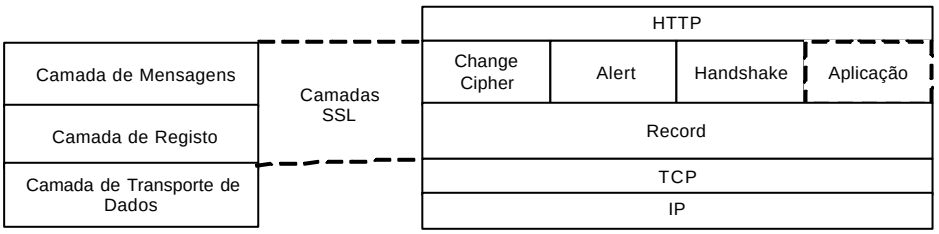


Figura 2.27 Esquema de utilização do SSL/TLS

Os certificados desempenham um papel central para todos os serviços de autenticação e gestão das chaves oferecidas pelo SSL/TLS. Estes serviços dependem da ligação de uma entidade com a chave pública. O DNS é o elemento escolhido para a identificação do servidor de Web, embora não seja adequado para a identificação de utilizadores [SSLTLS99].

2.6.3 SET – *Secure Electronic Transactions*

O SET é uma especificação aberta de segurança concebida para proteger as transacções com o cartão de crédito através da Internet. A versão actual do SET, SETv1, emergiu de uma série de normas de segurança criadas pela *Mastercard* e pela *Visa* em 1996 [PKIIMES01].

O SET por si só não é um sistema de pagamento, é sim um conjunto de protocolos de segurança e de formatos que permitem que os utilizadores possam usar a actual infra-estrutura de pagamentos com cartões de crédito numa rede aberta, tal como a Internet, de uma forma segura. No essencial, o SET oferece três serviços:

- Um canal de comunicação seguro entre todas as partes envolvidas na transacção;
- Confiança através da utilização de certificados X.509v3;
- Privacidade, uma vez que a informação está apenas disponível para as partes envolvidas na transacção quando e onde for necessária [UPKICSDC99, NSEAS00].

Os requisitos que foram identificados para o SET são os seguintes:

- Proporcionar confidencialidade do pagamento e da informação da encomenda;
- Assegurar a integridade dos dados transmitidos;
- Proporcionar a garantia de que um detentor de um cartão de crédito é o utilizador legítimo de uma conta de cartão de crédito;
- Proporcionar a garantia de que um comerciante pode aceitar transacções com cartão de crédito através da sua relação com uma instituição financeira;
- Assegurar a utilização das melhores práticas de segurança e técnicas de desenho do sistema para protecção das partes legítimas numa transacção de Comércio Electrónico;
- Criar um protocolo que não dependa nem de mecanismos de segurança da camada de transporte nem que impeça a sua utilização;
- Facilitar e encorajar a interoperabilidade entre fornecedores de *software* e de tecnologias de rede.

As funcionalidades principais do SET podem resumir-se em:

- Confidencialidade da Informação;
- Integridade dos dados;
- Autenticação da conta de cartão de crédito;
- Autenticação do comerciante.

As principais entidades que fazem parte de uma arquitectura SET (Figura 2.28) são as seguintes:

- Detentor do Cartão de Crédito (*Cardholder*): um detentor autorizado de um cartão de crédito de pagamento;
- Comerciante (*Merchant*): pessoa ou organização que possui bens ou serviços para vender ao Detentor do Cartão de Crédito;
- Emissor do Cartão de Crédito (*Cardissuer*): instituição financeira que fornece o Cartão de Crédito ao Detentor;
- Processador de Compras (*Acquirer*): instituição financeira que estabelece uma conta com um Comerciante e que processa autorizações e pagamentos com o cartão de crédito;
- Processador de Pagamentos (*Payment Gateway*): função operada pelo *Acquirer* ou outra entidade terceira que processa as mensagens de pagamento do Comerciante;
- Autoridade de Certificação (*Certification Authority*): entidade de confiança que emite certificados X.509 para Detentores de Cartão de Crédito, Comerciantes e Processadores de Pagamentos.

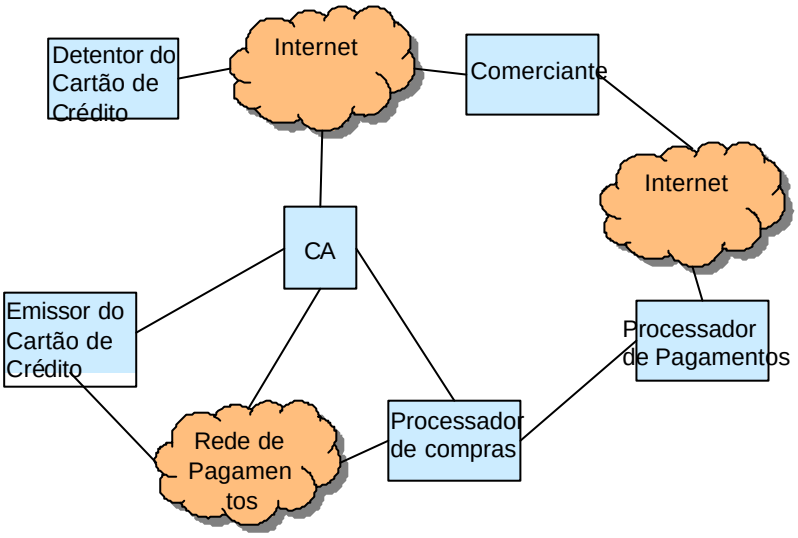


Figura 2.28 Arquitectura genérica do SET

Para processar uma transação SET são necessários diversos passos (Figura 2.29), os quais se descrevem de seguida [PKIIMES01]:

1. O Consumidor abre uma conta (num Banco, e solicita um cartão de crédito *Visa* ou *Mastercard*);
2. O consumidor recebe um certificado (X.509v3 assinado pelo Banco);
3. Os Comerciantes possuem os seus próprios certificados (dois certificados: um para assinaturas digitais de mensagens e outro para trocas de chaves; necessita ainda de uma cópia do certificado do Processador de Pagamentos);
4. O Consumidor coloca uma encomenda (envia os produtos a adquirir, o Comerciante devolve uma lista com os produtos e preços e o número da encomenda);
5. O Comerciante é verificado (o Comerciante envia uma cópia do seu certificado para o Consumidor);

6. A encomenda e o pagamento são enviados (é enviada informação da encomenda e de pagamento para o comerciante em conjunto com o certificado do cliente. A informação do pagamento é encriptado para que o comerciante não possa aceder à informação);
7. O Comerciante solicita uma autorização de pagamento (envia a informação de pagamento para o Processador de Pagamentos e requer a autorização de crédito);
8. O Comerciante confirma a encomenda:
9. O Comerciante envia bens e serviços para o Consumidor;
10. O Comerciante solicita pagamento através do Processador de Pagamentos.

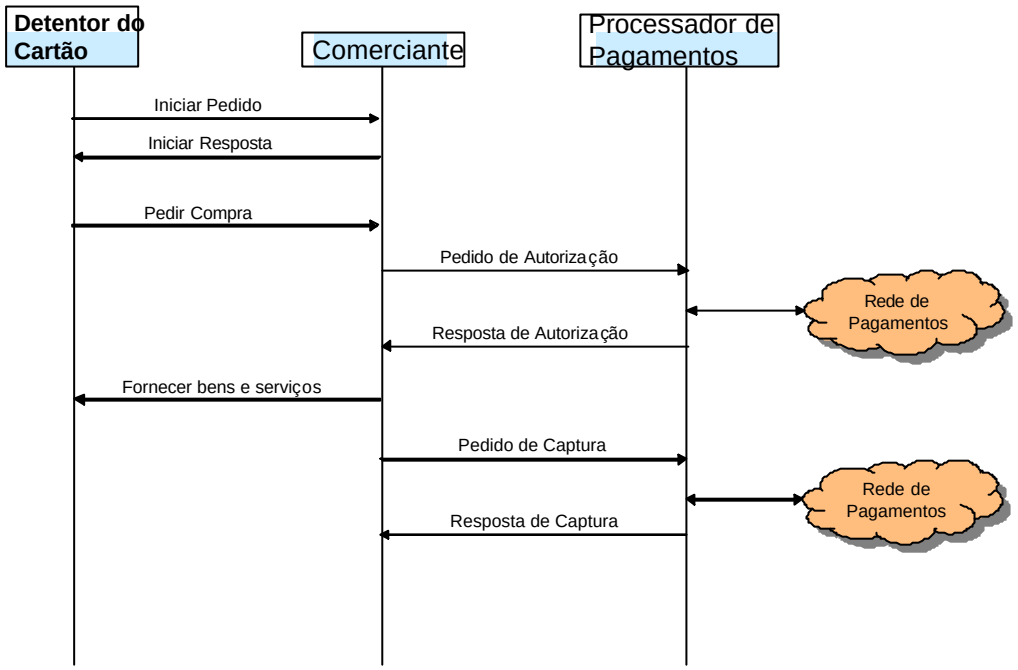


Figura 2.29 Processamento de uma transacção de pagamento SET

2.6.4 IPSec – *IP Security*

O IPSec proporciona segurança para os pacotes (datagramas) *Internet Protocol* (IP). Todo o tráfego Internet é processado através de datagramas IP. O IPSec é utilizado para proteger as comunicações entre máquinas ou entre as fronteiras das organizações [UPKICSDC99, NSEAS00]. O IPSec é o protocolo de segurança que é usado para implementar VPNs – *Virtual Private Networks*.

O IPSec permite a existência de comunicações seguras através de uma LAN, através de WANs privadas ou públicas e através da Internet. Alguns dos exemplos de utilização são os seguintes:

- Construção de VPNs sobre a Internet;
- Acesso seguro remoto através da Internet;
- Estabelecimento de conectividade através de Intranets e Extranets com parceiros;

- Melhoria de segurança do Comércio Electrónico [PKIIMES01].

A característica principal do IPSec, que permite o seu suporte a muitas aplicações, consiste no facto deste encriptar e autenticar todo o tráfego ao nível do IP.

A norma IPSec é bastante complexa e abrangente consistindo num conjunto de documentos (os mais importantes são RFC2401 [RFC2401], RFC2402 [RFC2402], RFC2406 [RFC2406], RFC2408 [RFC2408]). Estes documentos encontram-se divididos por diversos grupos:

- Arquitectura;
- ESP – *Encapsulating Security Payload*;
- AH – *Authentication Header*;
- Algoritmo de Encriptação;
- Algoritmo de Autenticação;
- Gestão de Chaves;
- Domínio de Interpretação.

O IPSec oferece diversos serviços de segurança na camada IP (Tabela 2.3) através de um mecanismo que permite seleccionar os protocolos de segurança, determinar os algoritmos a usar para os serviços, e criar as chaves necessárias para oferecer esses mesmos serviços. Dois protocolos são usados para oferecer segurança: um protocolo de autenticação designado por *Authentication Header* (AH), e um protocolo de encriptação e autenticação combinada, designada por ESP – *Encapsulating Security Payload* (ESP) [NSEAS00, RSALFAQ00].

	Authentication Header	***Encapsulating Security Payload* (encriptação)**	***Encapsulating Security Payload* (encriptação e autenticação)**
Controlo de Acessos	X	X	X
Integridade *Conectionless*	X		X
Autenticação da origem dos dados	X		X
Rejeição de pacotes repelidos	X	X	X
Confidencialidade		X	X
Confidencialidade do fluxo de tráfego		X	X

Tabela 2.3 Serviços do IPSec

O protocolo *Authentication Header* oferece integridade para o pacote individual IP e autentica a origem do pacote quer através do endereço IP quer através do nome do utilizador. O AH oferece integridade para as partes seleccionadas do cabeçalho IP em conjunto com o pacote da camada acima [NSEAS00, WSCRTS97].

O protocolo *Encapsulating Security Payload* pode oferecer confidencialidade, autenticação e integridade. O ESP oferece confidencialidade através da encriptação do *payload*. O ESP oferece autenticação e integridade usando um valor de verificação da integridade [UPKICSDC99, NSEAS00].

Com a utilização em larga escala do IPSec tiveram que ser desenvolvidos métodos automáticos para efectuar trocas de chaves criptográficas. O protocolo *Internet Key Exchange* (IKE) é um desses métodos automáticos utilizados no IPSec e é um protocolo de gestão de chaves bastante complexo [NSEAS00, RSALFAQ00].

Os certificados digitais desempenham um papel fundamental no IKE em que a autenticação depende da ligação entre uma identidade (DNS, IP, endereço de correio electrónico, DN) e uma chave pública.

2.7 Tendências de Futuro das PKI

O XML (*Extensible Markup Language*) é um dos desenvolvimentos tecnológicos mais importantes e recentes da Internet que veio permitir que esta se pudesse continuar a desenvolver e a crescer. O desenvolvimento do XML tem afectado igualmente os aspectos de segurança da própria Internet e, consequentemente, tem influenciado o desenvolvimento das próprias PKI [PACS00, SXMLKPKIS01, EXMLS01].

Um dos problemas mais importantes que se colocam às PKI nos nossos dias é a sua carência em termos de interoperabilidade [PKIIF01]. Com a proliferação de múltiplas arquitecturas, modelos e formatos de certificados, colocam-se alguns entraves à troca de informação de segurança entre PKI distintas.

Outro problema levantado diz respeito ao desenvolvimento de aplicações baseadas na Web em que foram encontrados novos requisitos aos quais as normas e especificações tradicionais das PKI não poderiam dar resposta na sua totalidade, particularmente no mais recente paradigma de computação distribuída, como é o caso dos *Web Services* [WSTXMLSS01, IMHONISSR99, WSWLAPKI99].

O XML é uma tecnologia que pode ajudar responder a alguns destes problemas de interoperabilidade e de novos requisitos das aplicações baseadas na Web e como tal uma série de normas e especificações estão a ser desenvolvidas, quer por parte do W3C, quer por parte de outros organismos privados (OASIS[18]), para responder a alguns destes problemas [MPKI96, CSSSEC00].

2.7.1 Codificação XML dos certificados SPKI

Este método permitiu a definição de forma normativa para codificação de certificados SPKI em XML, por oposição ao formato *S-Expression* tradicionalmente utilizado [WSTXMLSS01, XMLESPKIC00].

[18] http://www.oasis.com

Existem diversos motivos pelos quais o XML é uma boa escolha para codificar os certificados:

- Apesar de ser uma tecnologia recente, o XML tem sido facilmente adoptado. Existe uma grande quantidade de *software* que permite efectuar o processamento de XML;
- Mesmo os dispositivos pequenos tais como telemóveis WAP, telemóveis 3G ou PDAs podem possuir um processador XML;
- Existem duas API[19]s, substancialmente divulgadas, que podem ser utilizadas como interface com o processador XML: DOM - *Document Object Model* e o SAX – *Simple API for XML*;
- Os certificados XML podem ser verificados com definições DTD[20] usando um processador XML. A possibilidade de verificação automática torna fácil a verificação da construção dos certificados XML;
- XML é um formato legível por humanos e por sistemas informáticos. Isto torna os certificados mais explícitos para os utilizadores e programadores;
- Os documentos XML podem facilmente ser convertidos para diferentes formas de representação usando o XSL [XMLESPKIC00, SPKIXMLCS02].

Existe alguma objecção quanto ao tamanho dos certificados codificados em XML comparativamente com outros formatos binários. No entanto, isto não é um problema uma vez que o processamento dos certificados na validação da assinatura digital é, por si só, um processo lento. Para além disso, um dispositivo normal não irá tratar mais do que um pequeno número de certificados em simultâneo num determinado período de tempo [ASN1XML02].

Um aspecto importante nesta codificação refere-se ao facto de que os documentos XML deverem apenas conter dados textuais (ASCII). Assim sendo, todos os dados binários contidos num certificado devem ser re-codificados usando a codificação Base64. Por exemplo, as chaves públicas e os *hashs* (resumos) são objectos que contém informação binária e portanto devem ser codificados.

Um outro aspecto importante nesta codificação em XML é que as assinaturas devem usar o formato XMLDSig especificado pelo W3C (Secção 2.7.2).

2.7.2 Assinaturas Digitais em XML – *XML Digital Signature* (XMLDSig)

As assinaturas digitais em XML especificam a sintaxe XML e as regras de processamento para criar e representar assinaturas digitais. As assinaturas digitais em XML podem ser aplicadas a qualquer conteúdo digital (dados), incluindo o próprio XML [XMLSSP01].

A assinatura digital em XML é um método que permite associar uma chave com os dados referenciados. Não especifica como é que as chaves estão associadas com as pessoas ou com as instituições, nem qual o significado dos dados a serem assinados. Apesar desta especificação ser um componente importante na

[19] *Application Program Interface*

[20] *Document Type Definition*

construção de aplicações XML seguras, por si só não é suficiente para lidar com todas as preocupações de segurança/confiança das mesmas [XMLSSP01, EXMLS01].

2.7.3 Encriptação XML - *XML Encryption* (XMLEnc)

Esta norma especifica um processo para encriptação de dados e representação do seu resultado em XML. Os dados podem ser arbitrários, um elemento XML ou o conteúdo de um elemento XML. O resultado da encriptação dos dados é um elemento XML que contém ou identifica os dados cifrados [EXMLS01].

Esta especificação permite que documentos XML estejam apenas parcialmente encriptados, oferecendo assim protecção selectiva para os dados no documento XML que sejam efectivamente sensíveis.

2.7.4 XKMS - XML *Key Management Specification*

Esta norma (XKMS – Especificação XML para Gestão de Chaves) especifica um conjunto de protocolos para a distribuição e registo de chaves públicas, específico para a utilização em conjunto com XMLDSig e com o XMLEnc. É composto por duas partes distintas: XKISS (*XML Key Information Service Specification*) e o XKRSS (*XML Key Registration Service Specification*) [EXMLS01, WSTXMLSS01].

O XKISS define um protocolo para um serviço de confiança que resolve informação acerca de chave pública contida nos elementos das XMLDSig. O objectivo deste protocolo é o de minimizar a complexidade das implementações das aplicações de segurança, permitindo a utilização por parte destas de serviços PKI para o estabelecimento de relações de confiança de uma forma transparente. As PKI a serem utilizadas pode ser baseadas em modelos tradicionais tais como X.509/PKIX, SPKI ou PGP.

O XKRSS define um protocolo para os *Web Services* que aceita o registo de informação de chaves públicas. Uma vez registada, a informação de chave pública pode ser utilizada em conjunto com outros *Web Services* incluindo o próprio XKISS.

Ambos os protocolos são definidos em termos de estruturas XML usando os pacotes SOAP[21] para encapsular as mensagens de protocolo [XMLKMS01, EXMLS01].

2.7.5 As PKI e os *Web-Services*

Conforme já foi referido, o XML é um dos desenvolvimentos tecnológicos mais importantes e recentes da Internet que veio permitir que esta pudesse continuar a desenvolver e a crescer (com especial relevância para o novo paradigma dos *Web Services* (WS)). No entanto, existe ainda algum trabalho que necessita de ser realizado ao nível da segurança, para que todas as potencialidades destas tecnologias baseadas em XML possam ser utilizadas. Actualmente é possível encriptar um documento em XML, verificar a sua integridade e autenticidade do emissor, sendo este um processo relativamente simples. No entanto, torna-se cada vez mais necessária a utilização destas funções em partes de documentos, para encriptar e autenticar

[21] *Simple Object Access Protocol*

sequências arbitrárias, e para envolver diferentes utilizadores. Actualmente existem algumas especificações na área da segurança do XML: XMLEnc, XMLDSig, SAML e XKMS [XMLKMS01, EXMLS01].

O XML tornou-se muito rapidamente num mecanismo útil para trocar informação através da Internet. Tecnologias como o SOAP facilitam de certa forma a troca dessas mensagens XML através da Internet, o UDDI[22] está a desenvolver uma especificação que permite a aproximação de clientes e fornecedores de WS e o WSDL[23], que permite a descrição desses mesmos WS [XMLKMS01, EXMLS01].

Outra das áreas de grande desenvolvimento é a da segurança. No entanto, a adopção de alguns dos paradigmas da segurança e das próprias PKI não tem sido um processo fácil. Têm sido várias as entidades que se têm debruçado sobre esta complexidade e que têm dado origem a uma série de especificações [XMLKMS01, EXMLS01]:

- XMLEnc;
- XMLDSig;
- XACL – *eXtensible Access Control Language*;
- SAML – *Security Assertion Markup Language* (mistura AuthML e S2ML);
- XKMS – *XML Key Management Specification*.

Os *Web Services* são aplicações modulares, auto-contidas, que podem ser descritas, publicadas, localizadas e invocadas através da Internet. Podem desempenhar desde funções muito básicas e simples até funcionalidades mais avançadas e complexas como sejam a integração de processos de negócio [XMLKMS01].

Os WS vão ser utilizados na Internet, que pela sua natureza é insegura, e isto pode apresentar alguns riscos na realização de transacções críticas para as organizações, que necessitam de uma arquitectura que deverá contemplar os seguintes aspectos: Autenticação, Autorização, Confidencialidade, Integridade e Não-Repúdio (Figura 2.30).

[22] *Universal Description, Discovery and Integration*

[23] *Web Services Description Language*

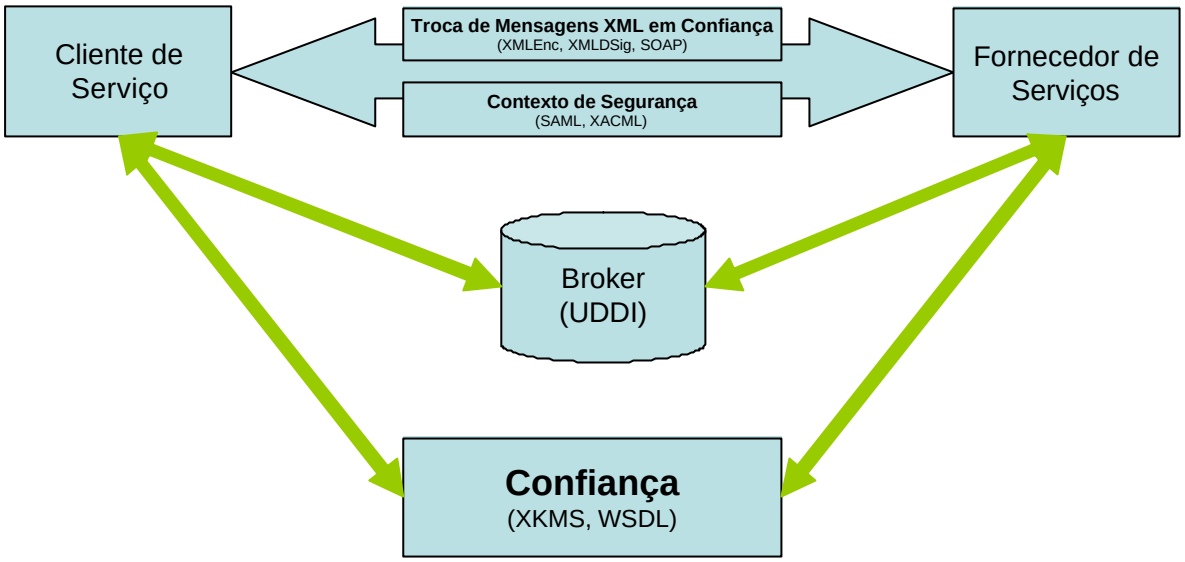


Figura 2.30 Arquitectura de Segurança XML para os *Web Services*

A interacção principal nos WS é a transmissão de mensagens entre os clientes e os fornecedores de serviços. As mensagens são tratadas em XML, encapsuladas em envelopes SOAP e transmitidas com o protocolo de transporte HTTP (Figura 2.30). As especificações de segurança nesta camada são: XMLEnc e as XMLDSig [XMLKMS01, EXMLS01].

O desenvolvimento de aplicações tem tido cada vez mais ênfase em aspectos de segurança. No entanto a integração de aplicações com capacidades PKI não é fácil e por vezes a interoperabilidade entre os próprios produtos de PKI é praticamente inexistente.

O Serviço de Estabelecimento de Confiança (Figura 2.30) é por si só um WS que os restantes WS podem invocar para permitir o estabelecimento da confiança nas suas transacções. Este Serviço de Estabelecimento de Confiança é o responsável pela criação da confiança necessária através de funções de segurança, tais como: assinaturas digitais, encriptação, *timestamping*, e as funções administrativas necessárias (registo, revogação e validação de chaves). Na verdade, o Serviço de Estabelecimento de Confiança não é mais do que um WS que disponibiliza as funções desempenhadas por uma PKI tradicional aos WS que necessitem delas. A especificação de segurança nesta camada é o XKMS [XMLKMS01, EXMLS01].

O estabelecimento de um contexto de confiança é o conjunto de informação adicional que deve ser apresentada entre o cliente e o fornecedor de serviços de forma a suportar transacções de negócio de confiança [XMLKMS01, EXMLS01].

O presente capítulo apresentou de uma forma compreensiva o estado-da-arte das PKI. Foi realizada uma investigação profunda com o intuito de cobrir da forma mais completa possível todos os aspectos relacionados com as PKI. Após a finalização deste estudo é possível tirar algumas conclusões importantes, nomeadamente que:

- No actual contexto do comércio electrónico a segurança é fundamental;

- As PKI são essenciais para os mecanismos de segurança funcionarem a uma escala global;

- As PKI são essenciais para estabelecimento de confiança entre os diversos intervenientes;

- Existe um domínio claro por parte do X.509 na implementação das PKI;

- A arquitectura com maior representatividade é o PKIX;

No entanto, tecnologias como o XML vão introduzir mudanças no seio do desenho das PKI e novos formatos vão surgir.

Veremos nos próximos capítulos desta dissertação a forma como as PKI podem ser utilizadas num contexto muito particular, neste caso no Comércio Electrónico de conteúdos digitais, e de que forma é as suas funcionalidades podem ajudar a solucionar alguns dos problemas desse tipo particular de Comércio Electrónico, nomeadamente:

Protecção do conteúdo digital;

Protecção dos pagamentos electrónicos;

Estabelecimento de confiança entre os diversos intervenientes nas relações electrónicas;

Protecção e Gestão dos direitos de autor.

3 A OPIMA E O OCCAMM

3.1 Introdução

De acordo com alguns dos estudos realizados pela *Forrester Research*, as empresas de produção de conteúdos prevêem que cerca de 20% das suas receitas irão ser obtidas através dos seus negócios *on-line* [SGDD00, TCFMI00]. No entanto, as companhias discográficas prevêem que irão perder cerca de 3.1 biliões de dólares e os editores cerca de 1.4 biliões de dólares uma vez que os consumidores recorrem cada vez mais à pirataria e os artistas se tornam mais e mais independentes. Apenas cerca de 50% destas empresas criaram parcerias para a aplicação de tecnologia para salvaguarda de direitos digitais. As empresas de produção de conteúdos demonstram cada vez mais as suas preocupações face às situações de desrespeito dos direitos de autor nesta era digital, em que a maior parte das vezes o prevaricador nem é identificado nem sofre qualquer tipo de sanção [DMPP01].

O crescimento da procura de conteúdos digitais tem provocado um aumento no número de utilizadores legítimos. No entanto, o número de utilizadores ilícitos cresceu de igual forma podendo-se apontar como exemplos destes os utilizadores de tecnologias *peer-to-peer* (P2P) usadas para trocar ficheiros entre utilizadores através da Internet. O *Napster*[24], o *Audio Galaxy*[25] e o *KaZaA*[26] são exemplos reais da utilização abusiva deste tipo de tecnologia para trocar conteúdo digital [CPYGMSW01] (música, vídeos, *software*, livros, entre outros) sem quaisquer reservas relativamente à salvaguarda dos direitos de autor [DMPP01]. Igualmente, o desenvolvimento de novos formatos digitais como o MP3[27] (para áudio) ou DivX (para vídeo) facilita bastante a troca de cópias digitais de elevada qualidade através da Internet [NEMD00].

Existem vários exemplos em que o desrespeito pelos direitos de autor é uma realidade, como é o caso do processo movido pelo grupo musical *Metallica* aos utilizadores do *Napster* e à própria empresa *Napster*, por cópia e distribuição ilegal das suas músicas em formato MP3 [NEMD00]. Pode não parecer um problema muito importante, pois o grupo continua a vender os seus CDs por todo o mundo, mas quando analisamos o número de utilizadores do *Napster*, é fácil perceber o mercado potencial que pode ter sido perdido pelo grupo e correspondentes editoras. O que é mais perturbador é que, na maior parte dos casos, o infractor dos direitos de autor consegue efectuar cópias perfeitas (100% iguais ao original, sem qualquer perda de qualidade), e distribuí-las livremente através Internet, sem quaisquer motivos de preocupação de acção judicial. Isto é apenas possível pela ineficiência, quer de meios técnicos de protecção, quer pelo próprio

[24] http://www.napster.com

[25] http://www.audiogalaxy.com

[26] http://www.kazaa.com

vazio legal que actualmente existe, levando a que este tipo de medidas se torne uma necessidade crescente [TGFMI00].

A Gestão dos Direitos de Autor de Conteúdos Digitais levanta actualmente um dos maiores desafios para a comunidade dos conteúdos digitais [CP2PB2B00]. A gestão de direitos digitais de bens físicos beneficia da sua própria existência física inerente, uma vez que esta fornece uma barreira natural contra a exploração não autorizada do conteúdo. No entanto, mesmo depois de algumas iniciativas legislativas, existem lacunas na lei de direitos de autor pelo facto que os conteúdos em formato digital podem ser facilmente copiados e transmitidos através de modernas redes de comunicação [TCFMI00].

Com o crescimento da procura pelos sistemas de protecção dos direitos de autor e da segurança de conteúdos que permitam a comercialização efectiva de todos os tipos de material multimédia (que podem variar desde um simples texto até uma cena de vídeo mais complexa) e, ao mesmo tempo, por uma crescente interoperabilidade global de dispositivos de consumo e de material comercializado, o sucesso deste tipo depende do suporte fornecido pela conjunção coerente de arquitecturas abertas e de tecnologias proprietárias [TCFMI00].

As grandes empresas da indústria de conteúdos começam hoje a encarar com seriedade novos modelos de negócio, que passam por incorporar a Internet como um novo canal de divulgação e distribuição para os mesmos. No entanto, todas elas querem de alguma forma salvaguardar os seus direitos sobre os conteúdos que distribuem e comercializam (pois só assim garantem o retorno financeiro) [DMPP01].

Esta não é, no entanto, uma tarefa fácil. O que se verifica é que alterações à forma como é realizada a distribuição e partilha de conteúdos de forma ilegal na Internet não são aceites com facilidade, quer pelos utilizadores, quer pelos próprios autores e produtores de conteúdos, como se pode constatar pelo novo modelo que foi proposto pelo *Napster* [NEMD00, MP3BMD00].

São várias a iniciativas que têm vindo a ser discutidas e desenvolvidas pelos actores mais importantes neste sector. Uma destas iniciativas[28] teve início em 1998 e designava-se por OPIMA (*Open Platform Initiative for Multimedia Access*), cuja versão mais recente foi actualizada em 2001 (versão 1.1) [OPIMASP00].

Este capítulo descreve a iniciativa OPIMA e a implementação da mesma levada a cabo pelo projecto europeu OCCAMM[29]. A iniciativa OPIMA, na qual participei em algumas das reuniões, juntou um consórcio de parceiros académicos e industrias e especificou uma plataforma para o consumo seguro de conteúdo multimédia. O projecto OCCAMM, no qual participei igualmente, reuniu um consórcio de vários parceiros a nível europeu sob a alçada do programa IST[30] da União Europeia (UE). Este projecto visava a realização da primeira implementação da plataforma especificada pela iniciativa OPIMA e a sua integração com alguns componentes adicionais para a operação da mesma. No decorrer do projecto OCCAMM foram igualmente realizados testes de utilização real a todos os componentes desenvolvidos de forma a validar a implementação dos mesmos. Este capítulo descreve igualmente o trabalho realizado por este projecto.

---

[27] De facto, trata-se de MPEG-1/2 Layer 3

[28] Patrocinada pelo programa ITA – *Industry Technical Agreement* do IEC – *International Electrotechnical Commission*

[29] *Open Components for Controlled Access to Multimedia Material*

[30] *Information Society Technologies*

Na secção seguinte é apresentada uma descrição sucinta da iniciativa OPIMA para uma compreensão mais fácil dos objectivos da mesma.

3.2 A iniciativa OPIMA

A iniciativa designada por OPIMA especifica uma arquitectura que permite o descarregamento seguro, instalação e execução de sistemas de protecção proprietários, designados por sistemas IPMP (*Intellectual Property Management and Protection* – Gestão e Protecção da Propriedade Intelectual), que implementam a política de protecção específica do fornecedor de serviços e conteúdos no terminal do utilizador final [OPIMASP00]. A especificação desenvolvida pela iniciativa OPIMA, de forma a proporcionar este tipo de funcionalidades, especifica um SAC (*Secure Authenticated Channel* – Canal Seguro e Autenticado) e as interfaces apropriadas entre os sistemas IPMP e as aplicações dos utilizadores finais [SDDFT98]. A comunicação entre estas aplicações e os sistemas IPMP são realizadas através da OVM (*OPIMA Virtual Machine* – Máquina Virtual OPIMA), um elemento nuclear na arquitectura da iniciativa OPIMA. Esta iniciativa define apenas as interfaces entre a OVM e as aplicações e os sistemas IPMP, não especificando quaisquer detalhes acerca da implementação dos mesmos [OPIMASP00].

A OPIMA especifica uma plataforma modular em que os fornecedores de serviços possam ter a possibilidade de alargar o conjunto potencial de consumidores [OPIMASP00]. Da mesma forma, os consumidores passam a ter a possibilidade de aceder a uma grande variedade de conteúdos e fornecedores de serviços num contexto de sistemas múltiplos de protecção de conteúdo. Suporta um conjunto de serviços base e modelos tais como [OPIMASP00, SDDFT98]:

- Serviços de Subscrição de Áudio e Televisão;
- Pagar para Utilizar (*Pay-per-Use*);
- Vídeo e Áudio a pedido;
- Serviços que acrescentem valor aos serviços mencionados anteriormente – por exemplo, através de EPGs[31] seleccionados e outros serviços afins (Figura 3.1);
- Serviços multimédia *on-line* – tais como o consumo de serviços através da Internet;

[31] EPG – *Electronic Program Guide*

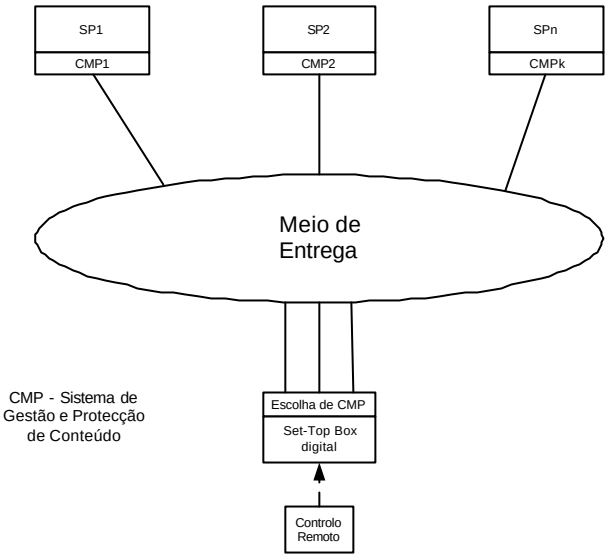


Figura 3.1 O conceito da especificação da iniciativa OPIMA

A especificação desenvolvida pela iniciativa OPIMA é totalmente independente de dispositivos e do conteúdo, definindo uma arquitectura P2P – *Peer to Peer*. Uma arquitectura P2P difere de uma arquitectura tradicional cliente-servidor, uma vez que enquanto nesta última um dos elementos desempenha estritamente o papel de cliente e o outro de servidor, na arquitectura P2P ambos podem ser em simultâneo cliente e servidor [OCFDOVM00, OPIMASP00]. O seu principal objectivo foi a definição de uma plataforma capaz de proteger e gerir qualquer tipo de conteúdo digital. A protecção e a gestão do conteúdo são realizadas através da utilização de sistemas de protecção (ver secção 3.2.1) e de regras aplicados a cada um dos conteúdos (ambos podem ser descarregados para a plataforma de protecção).

Este sistema de protecção, designado por sistema IPMP é um *software* proprietário que pode ser descarregado de forma segura para uma plataforma OPIMA e cujo objectivo é o de descodificar e forçar a aplicação das regras de utilização sobre o conteúdo. O sistema IPMP pode libertar ou não as chaves necessárias para desencriptar o conteúdo, actuando assim como uma guarda avançada de qualquer arquitectura de segurança baseada na iniciativa OPIMA [OCFDOVM00].

3.2.1 Componentes da OPIMA

A plataforma definida pela iniciativa OPIMA é composta por três componentes fundamentais: a Máquina Virtual OPIMA (OVM) e duas APIs (API de Serviços da Aplicação e API de Serviços do Sistema IPMP) [OPIMASP00, OCFDOVM00]. Esta plataforma é descrita na figura seguinte (Figura 3.2):

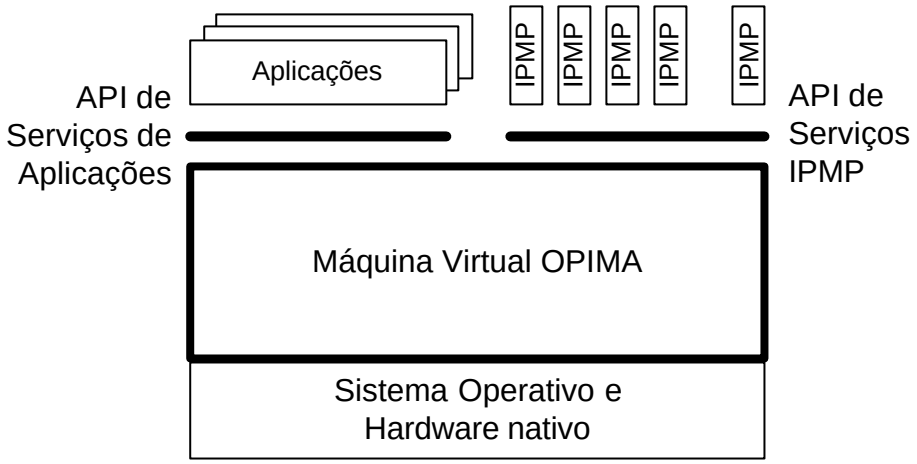


Figura 3.2 Plataforma da iniciativa OPIMA

A OVM é o componente nuclear da plataforma OPIMA e funciona como uma "caixa negra" [OPIMASP00], no sentido em que os seus componentes não podem ser modificados, depois da plataforma individual OPIMA ser certificada. Esta OVM pode ser composta por diversos componentes, nomeadamente:

- Codificadores e Descodificadores (CODEC) de um determinado tipo de conteúdo[32]. Uma OVM poderá ter mais que um CODEC tornando possível usar mais que um único tipo de conteúdo;
- Bibliotecas de encriptação e desencriptação que podem implementar diversos tipos de algoritmo[33];
- Bibliotecas de assinaturas digitais, podendo igualmente implementar diversos algoritmos;
- Bibliotecas de introdução e monitorização de marcas de água, com a possibilidade de implementação de diversos algoritmos[34];
- Módulos de extracção de regras, que são utilizados a pedido do sistema IPMP;
- Um conjunto de protocolos OPIMA, necessários para estabelecer a comunicação entre plataformas OPIMA, e descarregamento seguro de sistemas IPMP.

Enquanto que o último dos componentes especificados é absolutamente necessário em qualquer implementação de uma plataforma OPIMA, os outros são opcionais (de acordo com a especificação). Uma característica importante de cada plataforma OPIMA é a capacidade de estabelecer um *Secure Authenticated Channel* (SAC) com outro *peer* OPIMA [OCCSTOP00, OCFDOVM00]. O objectivo principal do SAC é o de permitir o descarregamento seguro de sistemas IPMP sempre que tal se revele necessário, podendo igualmente ser utilizado para que sistemas IPMP instalados em diferentes OVMs possam trocar dados em segurança entre si. Esta capacidade é responsável por uma característica importante da especificação desenvolvida pela iniciativa OPIMA: a interoperabilidade. Esta especificação, define o

[32] A actual implementação da OVM, levada a cabo pelo projecto OCCAMM possui um CODEC (Codificador/Descodificador) MPEG-4 integrado

[33] Da mesma forma, os algoritmos implementados são o AES, RSA com MD5 e RSA com SHA1

protocolo SSL/TLS como a tecnologia escolhida para estabelecer o SAC, no entanto, a especificação refere que outros tipos de tecnologias, proprietárias ou não, podem ser utilizadas para o estabelecimento do SAC [OCCSTOP00].

Cada plataforma OPIMA possui uma credencial que é utilizada para estabelecer o SAC, criando um ambiente seguro o que permite que um fornecedor de conteúdo possa confiar numa OVM e enviar os seus sistemas IPMP para serem executados sob o controlo da OVM [OCCSTOP00, OCASASFD00].

Esta característica proporciona um grau significativo de independência entre os diversos fornecedores de conteúdo, os seus fornecedores de segurança e os fornecedores de plataformas OPIMA.

Os outros dois elementos fundamentais da plataforma OPIMA são duas APIs: a API de Serviços para Aplicações e a API de Serviços para Sistemas IPMP. A API de Serviços para Aplicações é utilizada pelas aplicações, que possuem algum interface para comunicar com o utilizador. Esta API é implementada pela plataforma OPIMA e fornece os pontos de entrada para uma aplicação. A pedido do utilizador, uma aplicação pode invocar um conjunto de métodos da API, tais como: interrogar a OVM, descarregar um determinado sistema IPMP, enviar mensagens para um determinado sistema IPMP e enviar instruções para a OVM utilizar o conteúdo. Baseada numa resposta da OVM, a aplicação pode perguntar ao utilizador para seleccionar um sistema IPMP previamente descarregado, ou pedir à OVM para descarregar e executar um novo sistema IPMP específico para o conteúdo. A única especificação normativa na iniciativa OPIMA é a API, e nada é especificado para a aplicação, que pode ter qualquer tipo de interface com o utilizador (*browser* de *Web*, controlo remoto de televisão, entre outros) [OCASASFD00].

A API de serviços IPMP será utilizada pelos sistemas IPMP. Esta API proporciona um conjunto de métodos que permitem que os sistemas IPMP possam aceder às regras de conteúdo, às regras de utilização, às capacidades de encriptação e desencriptação da OVM, às bibliotecas de assinatura digital e de introdução de marcas de água, às interfaces de cartões inteligentes, comunicação com o utilizador, com a aplicação ou com sistemas de IPMP. As regras de conteúdo, são dados que se encontram embebidos directamente no conteúdo e que indicam qual o tipo de protecção do mesmo (indicação do sistema IPMP que o protege, tipo de protecção, entre outros). As regras de utilização, são regras que são obtidas à posteriori pelo sistema IPMP e que controlam a forma como o utilizador pode aceder e controlar o conteúdo. Devem ser flexíveis e contemplar os seguintes aspectos, entre outros [IDRM02]:

- **Limites de utilização**: em que se pode especificar o número de vezes o utilizador pode aceder a um determinado conteúdo;
- **Limite de utilização por dispositivo**: a possibilidade ligar um determinado conteúdo a um dispositivo específico para que possa apenas ser visualizado neste;
- **Controlo de armazenamento e de transferência**: permite controlar o número de vezes que um conteúdo protegido pode ser armazenado noutro meio;
- **Limites de Calendário**: o conteúdo pode ser licenciado com base numa data, ou hora do dia;

[34] O algoritmo INTAGLIO foi implementado nesta OVM

- **Pré-utilização sem licença**: mesmo que o utilizador não tenha adquirido uma licença para visualização do conteúdo, o fornecedor do mesmo pode fornecer uma licença que permite uma pequena visualização do mesmo;
- **Super-distribuição**: refere-se ao facto de os utilizadores poderem redistribuir o conteúdo para outros utilizadores;
- **Acesso Granular**: permite controlar o acesso a partes específicas do conteúdo mantendo as restantes protegidas.

O conteúdo é processado pela OVM, no entanto é o sistema IPMP que decide se um determinado utilizador possui os direitos necessários para realizar uma determinada acção solicitada [OCISAFD00]. A decisão é tomada pelo código proprietário do sistema IPMP baseado nas regras de conteúdo e nas regras de utilização. No caso do utilizador possuir os direitos apropriados, o sistema IPMP irá fornecer as chaves necessárias à OVM, ou os meios para as obter, que irão permitir a desencriptação do conteúdo. Existem momentos em que diversos sistemas IPMP podem ser executados em simultâneo num ambiente de multi-tarefa gerido pela OVM [OCISAFD00].

A especificação da iniciativa OPIMA aponta para o desenvolvimento e utilização de diferentes modelos de negócio, que podem ser implementados pelas diversas plataformas OPIMA com as características específicas de cada um [OCBMS00].

3.2.2 Protocolos OPIMA e a Interoperabilidade

Os protocolos OPIMA são protocolos que permitem o estabelecimento de SACs, assim como a execução de sistemas IPMP na OVM. Protocolos proprietários podem ser utilizados para obter a mesma funcionalidade entre diversos *peers* OPIMA dentro de um determinado compartimento [OPIMASP00]. A comunicação entre os diversos sistemas IPMP instalados nos diversos *peers* OPIMA pode ser efectuada utilizando protocolos proprietários, que funcionam sobre os protocolos base da iniciativa OPIMA. Estes protocolos são necessários para proporcionarem um certo nível de interoperabilidade entre os *peers* OPIMA estando divididos em dois níveis:

(1) um primeiro nível, designado por nível de transporte seguro, que negoceia e implementa o SAC. Para este nível a iniciativa OPIMA especificou o SSL/TLS como sendo o protocolo de referência para comunicações seguras entre compartimentos, servindo para o estabelecimento de mecanismos de encriptação e desencriptação a serem utilizados pelas OVM, para transmitir de forma segura os sistemas IPMP entre dois *peers* em comunicação [OCCSTOP00].

(2) o segundo nível, designado por Protocolo de Mensagens Comum OPIMA (CMP - *Common Message Protocol*), utiliza a funcionalidade proporcionada pelo nível anterior. As mensagens trocadas através deste protocolo permitem o descarregamento de sistemas IPMP. As mensagens deste protocolo são constituídas por um comando e por parâmetros opcionais. Estes parâmetros aparecem descritos na tabela seguinte [OCCSTOP00].

Emissor	Mensagem	Destinatário	Descrição

Peer 1	OPEN(8 bits), tamanho(8 bits), IPMPS_ID(variável)	*Peer* 2	Mensagem de início de descarregamento do sistema IPMP
Peer 2	MSGDATA(8 bits), tamanho(32 bits), mensagem (variável)	*Peer* 1	Mensagem de descarregamento do sistema IPMP
Peer 2	CLOSE (8bits)	*Peer* 1	Mensagem de fim de descarregamento do sistema IPMP.
Peer 1	CLOSE (8bits)	*Peer* 2	

Tabela 3.1 Mensagens do Protocolo CMP

3.2.3 OPIMA e Modelos de Negócio

O conjunto de interacções seguras entre as diversas OVM representa o ambiente OPIMA. No entanto, as OVM não necessitam de estar permanentemente ligadas ao resto do ambiente OPIMA. Uma OVM pode funcionar de forma ligada e/ou de forma desligada, permitindo assim diversos modelos de negócio [OCBMS00]. Alguns dos possíveis exemplos da flexibilidade dos modelos de negócio são:

1. Possibilidade de utilizar a mesma plataforma para poder usufruir de diferentes tipos de conteúdo provenientes de um fornecedor de serviço: supondo que os consumidores adquirem o seu dispositivo multimédia que integra uma OVM, esta possui a possibilidade de mostrar conteúdos que podem ser de diferentes tipos: áudio, vídeo, imagens, entre outros – claro que a OVM terá que possuir o descodificador apropriado para o conteúdo em causa;

   Por exemplo, o *Microsoft Windows Media Player*, com uma OVM integrada pode ser usado para visualizar uma emissão de vídeo em formato AVI do programa *BigBrother* da TVI e uma animação de *Macromedia Flash* do *site* de Web igualmente da TVI.

2. Possibilidade de utilização da mesma plataforma para poder usufruir de conteúdo proveniente de dois fornecedores diferentes: com a mesma OVM, o utilizador pode usar os conteúdos provenientes de um fornecedor de serviços A (SPV_a) e de um fornecedor de serviços B (SPV_b);

   Por exemplo, o *Microsoft Windows Media Player*, com uma OVM integrada pode ser usado para visualizar jogos de futebol emitidos pela *SportTV*, assim como jogos de futebol emitidos pela RTP1, em formato MPEG-2.

3. Possibilidade de um fornecedor de conteúdos recorrer a dois fornecedores de segurança distintos para proteger o seu conteúdo: em que um dado conteúdo K, fornecido por um determinado fornecedor de serviços A (SPV_a) recorre a um fornecedor de segurança S (FS_S) e a outro T (FS_T);

   Por exemplo, a TvCabo recorre a dois sistemas de segurança distintos, um baseado nas *TvBox* sem cartões inteligentes e outro baseado em cartões inteligentes.

4. Possibilidade de um determinado fornecedor de serviços poder especificar que o seu conteúdo apenas poderá ser utilizado uma determinada implementação da OVM e não em outra;

> Por exemplo, a TvCabo estabelece um acordo com a *Microsoft* e faz com que os conteúdos que fornece apenas possam ser visualizados pela implementação da OVM da Microsoft e não por implementações de OVMs de fabricantes distintos.

A última versão da especificação da iniciativa OPIMA (versão 1.1) [OPIMASP00] e os esforços de implementação iniciais levados a cabo pelos vários parceiros de um projecto Europeu designado por OCCAMM[35] (como será apresentado na secção seguinte), provaram que a normalização e operação de tal arquitectura é uma tarefa relativamente complexa, mas possível. No entanto, esta arquitectura necessita de especificar ainda um determinado número de entidades, tais como autoridades de registo e de certificação suportadas por uma PKI, tal como se encontra referido de seguida (ver ponto 4.1.2). A iniciativa OPIMA especifica muito pouco do ponto de vista destas entidades e das credenciais emitidas por estas, referindo apenas a necessidade de existência das mesmas [OPIMASP00]. Este será um dos objectivos de trabalho da presente dissertação de Mestrado em que uma PKI funcional irá ser proposta (ver Capítulo 4).

3.2.4 Os certificados digitais e a iniciativa OPIMA

A emissão e utilização de credenciais ou certificados digitais na especificação criada pela iniciativa OPIMA é necessária, mas não se encontra devidamente especificada. Estas credenciais são necessárias para [OCCSTOP00]:

- Certificação do número único de identificação de cada compartimento;
- Certificação das implementações da OVM, através da atribuição a cada OVM individual de um número único de identificação;
- Certificação das diversas implementações de cada sistema IPMP, através da atribuição de números de identificação únicos que serão utilizados para referenciar os sistemas IPMP para descarregamento;
- Registo de algoritmos de encriptação, assinatura digital e inserção de marcas de água para que as OVM e os sistemas IPMP possam partilhar identificadores comuns.

Tal como foi referido, as autoridades de emissão de certificados não se encontram identificadas na iniciativa OPIMA. No entanto, é identificada a clara necessidade da existência de instituições que irão emitir e gerir os diversos identificadores e certificados necessários, que foram apontados anteriormente, principalmente nos aspectos que dizem respeito à renovação da segurança e revogação de direitos, conformidade de OVMs,

[35] OCCAMM – *Open Components for Controlled Access to Multimedia Material*, é um projecto no contexto do programa Europeu IST (IST-1999-11443)

aplicações e sistemas IPMP. Estas instituições podem ser públicas ou privadas, respeitando regras comuns de sociedade e de mercado [OPIMASP00].

Assim, a iniciativa OPIMA aponta como necessárias as seguintes instituições:

Autoridade de Emissão de Identificadores Únicos de Compartimento: cada compartimento deverá ser unicamente identificado. Uma autoridade deverá estar a cargo da emissão destes identificadores de compartimento.

Autoridades de Emissão de Credenciais: as credenciais OPIMA serão emitidas por autoridades de certificação OPIMA neutrais, que certificam implicitamente a natureza da implementação da OVM e do dispositivo no qual reside, assim como as suas capacidades.

Autoridades de Emissão de Identificadores Únicos de sistemas IPMP: os sistemas IPMP necessitam de estar identificados unicamente de forma a permitir a interacção segura entre os mesmos. Empresas ou organizações podem obter a permissão para emitirem identificadores de sistemas IPMP dentro de um determinado identificador único atribuído por estas autoridades.

Autoridade de Emissão de Identificadores Únicos do *Peer* OPIMA: os *peers* OPIMA precisam de ser identificados univocamente de forma a possibilitar a interacção segura entre eles. Empresas ou organizações podem obter a permissão para emitirem identificadores de *peers* OPIMA dentro de um determinado identificador único atribuído por estas autoridades.

Autoridade de Emissão de Identificadores Únicos para Algoritmos de Encriptação, Assinatura Digital e Inserção de Marcas de Água: algoritmos de Encriptação, Assinaturas Digitais e Introdutores de Marcas de Água precisam de ser identificados univocamente de forma a permitir que sistemas de IPMP e OVMs possam comunicar seguramente entre si.

Infra-estrutura de Apoio: em conjunto com os componentes funcionais nos dispositivos OPIMA, pode ainda existir uma interface com sistemas de processamento de apoio. Entre estes podem destacar-se instituições financeiras e de negociação de direitos de utilização. A estrutura destes componentes é perfeitamente proprietária, no entanto, estes irão utilizar *peers* OPIMA de forma a efectuarem a ligação com o ambiente OPIMA.

A iniciativa OPIMA defende a utilização da norma de certificados X.509v3 como credenciais. A identificação do compartimento e a identidade dos *peers* OPIMA é incluída na credencial. Esta credencial OPIMA deve obedecer ao formato X.509v3 em que o campo 'Subject' está formatado para que a estrutura contenha dois campos: CompartmentID e PeerID. O campo 'Issuer' contém a identificação da Autoridade que emitiu a credencial [OPIMASP00].

De uma forma genérica um certificado OPIMA é na verdade um certificado X.509v3 com os seguintes campos relevantes:

```
Certificate ::= SIGNED
{
        SEQUENCE {
        version         [0] Version DEFAULT v1,
        serialNumber    CertificateSerialNumber,
        signature       AlgorithmIdentifier,
        issuer          Name,
        validity        Validity,
```

```
        subject         Name,
        subjectPublicKeyInfo  SubjectPublicKeyInfo,
        issuerUniqueIdentifier [1] IMPLICIT UniqueIdentifier OPTIONAL,
                              -- if present, version must be v2 or v3
        subjectUniqueIdentifier [2] IMPLICIT UniqueIdentifier OPTIONAL
                              -- if present, version must be v2 or v3
        extensions              [3] Extensions OPTIONAL
                              -- If present, version must be v3 --
    }
}

issuer: IssuerID = OCTET STRING(2)
subject: SubjectID = SEQUENCE{CompartmentID OCTET STRING(4), PeerID OCTET STRING(16)}
```

3.3 O Projecto OCCAMM

A implementação e operação de uma plataforma OPIMA foram dois dos resultados mais importantes que foram obtidos no decorrer do projecto OCCAMM. Apesar desta plataforma constituir um demonstrador importante das capacidades da iniciativa OPIMA, outra das vertentes deste projecto era a demonstração da aplicabilidade da plataforma OPIMA através da realização de uma série de testes de utilização real [OCPH00]. Em resumo, o projecto OCCAMM realizou o desenvolvimento e teste de uma infra-estrutura de aplicações de comércio electrónico, baseadas na distribuição *on-line* de conteúdo digital multimédia, assim como na selecção e validação de modelos de negócio que dependem deste tipo de tecnologia, no contexto de inúmeros testes de utilização real levados a cabo com a colaboração de utilizadores finais [OCPH00, OCIMPATP01]. A arquitectura aberta de protecção e gestão de conteúdo que foi desenvolvida é compatível com algumas das especificações internacionais (OPIMA, SDMI[36] e MPEG IPMP), estabelecendo um elevado grau de portabilidade e interoperabilidade dos componentes de segurança, assim como a capacidade de implementação de políticas de marketing flexíveis. A combinação própria das tecnologias mais recentes e a validação de arquitecturas normalizadas é visto como o catalizador necessário para estimular a exploração do potencial da Internet, no campo da comercialização de conteúdos digitais pelos criadores de conteúdos, fornecedores de serviços e operadores de redes de comunicação, para benefício dos utilizadores finais. No entanto, deve ser realizado um esforço sério a nível Europeu para atingir massa crítica, quer em termos de competências técnicas, quer em termos de perícia negocial necessária para empreender tal objectivo ambicioso [OCPH00].

Em resumo, os principais objectivos do projecto OCCAMM foram:

- A especificação e desenvolvimento de um conjunto de ferramentas e componentes, compatíveis com normas abertas emergentes (OPIMA, SDMI, MPEG), que lidam com o acesso controlado, entrega, consumo e gestão dos direitos de informação multimédia;

- O estabelecimento de um conjunto de aplicações orientadas para o mercado que utilizam as ferramentas mencionadas no ponto anterior e que vão de encontro às necessidades dos fornecedores de serviço presentes ou emergentes no mercado;

[36] SDMI – Secure Digital Music Initiative, lançada no inicio de 1999 no seio da indústria da música com o objectivo de criar uma norma aberta para distribuição de musica digital *online*. A iniciativa está hoje em dia desactivada (http://www.sdmi.org).

- A definição e monitorização dos níveis de desempenho, em ambientes de teste, para as aplicações citadas anteriormente, e apontamento das acções adicionais necessárias para a subsequente bem sucedida exploração comercial [OCPH00].

3.3.1 Etapas do desenvolvimento do projecto OCCAMM

Para a implementação da arquitectura definida pela iniciativa OPIMA, o consórcio de parceiros OCCAMM optou pelo ambiente PC e pelos sistemas operativos Microsoft Windows. Embora este tipo de ambiente seja inerentemente inseguro, era suficiente para atingir os objectivos necessários do projecto. Esta implementação foi dividida em componentes distintos: a OVM, as duas APIs, a aplicação OCCAMM para mostrar conteúdo MPEG-4 (*player*) e o sistema IPMP. Mais, toda a infra-estrutura de suporte do teste teve igualmente de ser desenvolvida de raiz e algumas das infra-estruturas já existentes tiveram de ser adaptadas [OCPH00]. Em termos globais, teve que ser desenvolvida uma solução *Digital Rights Management* (DRM) que deveria suportar funcionalidades tão diversas [ODRM00] tais como:

- Gestão de termos e de condições de utilização;
- Protecção da integridade do conteúdo;
- Introdução de regras de comercialização específicas;
- Controlo sobre as regras de comercialização;
- Nível de protecção eficaz (Custo/Benefício);
- Segurança e confiança por parte dos intervenientes;
- Eficácia e flexibilidade nas formas de pagamento.

No entanto, o trabalho do OCCAMM acabou por centrar-se única e exclusivamente nos três primeiros aspectos relegando os restantes para segundo plano.

Todo o trabalho realizado ao longo do projecto OCCAMM pode ser resumido numa série de etapas que se encontram representadas graficamente e sucintamente descritas de seguida (Figura 3.3).

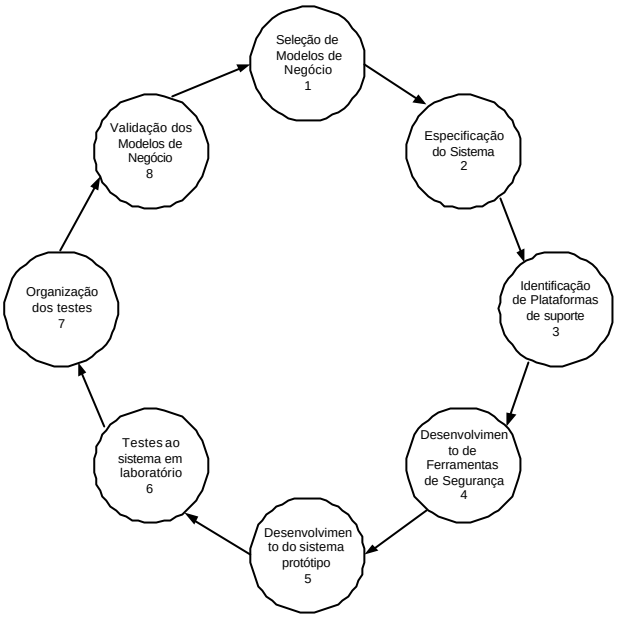


Figura 3.3 Etapas de desenvolvimento do projecto OCCAMM

Passo 1 – Selecção de modelos de negócio

Foi efectuada a análise de modelos de negócio tradicionais e emergentes para a distribuição de bens e serviços multimédia *on-line* em diversas áreas de aplicação (comercialização de música, livros, imagens, entre outros) e identificados aqueles que parecem ser os mais adequados para fazer face às expectativas dos utilizadores e promover o crescimento do mercado nessa área[37]. Um número de aplicações específicas voltadas para categorias de utilizadores bem definidos foram seleccionadas e os requisitos dos mesmos gerados para o sistema, de forma a proporcionar serviços de exemplo de acordo com o modelo de negócios definido [OCPH00].

Passo 2 – Especificar a implementação

Com base nos requisitos funcionais identificados no passo anterior, foram concebidas implementações particulares do sistema OCCAMM, que podiam suportar as aplicações exemplo identificadas. Estas implementações foram especificadas em termos de funcionalidades e de desempenho e os papéis dos subsistemas e componentes definidos de forma exacta, assim como as interfaces que permitiam interacções entre componentes. De forma a proporcionarem as funcionalidades chave, tecnologias relevantes recomendadas por instituições de normalização internacional foram seleccionadas e foi especificada a forma de utilização dos serviços oferecidos por plataformas comerciais [OCPH00].

Passo 3 - Desenvolvimento das Tecnologias necessárias

Com base na definição dos componentes de sistema, aqueles que ainda não existiam foram desenvolvidos de forma a proporcionarem os serviços e interfaces requeridas. Os esforços de desenvolvimento concentraram-se na implementação de tecnologias de controlo de acessos que representam uma parte essencial do sistema de segurança distribuído, permitindo a protecção e gestão do conteúdo de uma forma "*end-to-end*". Estes componentes são os elementos chave capazes de permitir a transformação dos modelos

de negócio teóricos numa plataforma capaz de validar os serviços orientados para o mercado, que sejam atractivos para os utilizadores finais e para os fornecedores de conteúdo [OCPH00].

Passo 4- Desenvolvimento e Teste da Plataforma

No laboratório foram desenvolvidos e testados diversos protótipos do sistema. Isto implicou a ligação de todos os subsistemas testados anteriormente que representam as várias entidades e verificar as diversas interacções. Igualmente, as diversas plataformas de serviços externas foram integradas nesta fase e a forma de exploração destes serviços foi definida. A partir daqui, testes funcionais e de depuração foram realizados até o sistema atingir um ponto de fiabilidade e desempenho considerado como adequado para fornecer o sistema a utilizadores externos [OCPH00].

Passo 5 – Realização de Testes de utilização

Os utilizadores foram seleccionados e convidados a participarem nos testes de utilização do sistema. Isto significa que pessoas, que não tinham qualquer conhecimento do desenvolvimento do sistema, utilizaram-no para fins profissionais ou privados. O OCCAMM tentou simular situações reais de fornecimento de serviços, baseados em material multimédia oferecido através de meios tradicionais e em aplicações que foram estruturadas de forma a serem o mais semelhante possível com o que seria o serviço real [OCPH00].

Passo 6 - Avaliação dos Resultados

Com vista a avaliar o grau de aceitação do sistema pelos utilizadores foi efectuada a recolha de opiniões dos mesmos de forma estruturada e organizada, o processamento dos resultados, a avaliação de dados críticos do sistema implementado e a identificação das vantagens e desvantagens do modelo de negócio seleccionado. Foi efectuada a validação do desempenho das tecnologias seleccionadas no fornecimento das funcionalidades solicitadas e a fiabilidade e robustez assegurada pelas soluções implementadas [OCPH00].

Como já foi referido anteriormente, o projecto OCCAMM levou a cabo uma diversidade de testes de utilização real com utilizadores finais como forma de validação da plataforma OPIMA desenvolvida e dos diversos modelos de negócio adoptados pelo consórcio. Mais precisamente, foram quatro os cenários de testes realizados [OCIOSF01, OCTRADR02]:

- Comercialização de música digital: em que faixas de música podem ser escutadas numa loja da Web e posteriormente adquiridas e descarregadas para o PC do utilizador. Podem depois ser tocadas sob o controlo da OVM e regras de licenciamento previamente definidas;

- Locução de Áudio: utilizadores que desejem criar locução de áudio para programas de TV, rádio, vídeo, CD-ROM, publicação na Web, entre outros, podem realizar esta operação completamente *on-line*, enviando o seu texto e negociando um contrato com o artista escolhido. Pode depois receber o ficheiro de voz para rever no seu PC, sob o controlo da OVM;

- *E-Learning*: conteúdo de aulas de Universidade foram publicadas em MPEG-4 e disponibilizadas através de uma LAN – *Local Área Network*, para que os estudantes pudessem aceder a este material mais tarde. O acesso e utilização deste conteúdo eram controlados pela OVM;

[37] Podem ser igualmente introduzidas algumas alterações em modelos de negócio existentes para que possam incorporar as funcionalidades oferecidas por tecnologias mais recentes

- Comercialização de imagens digitais: em que consumidores profissionais podiam navegar num *site* de comércio electrónico, escolhendo material fotográfico disponível e descarregar imagens em resoluções diferentes. Uma vez que o valor (preço) da imagem depende da resolução da mesma, a OVM, no PC do utilizador, controla o acesso a imagens de boa qualidade. A OVM irá igualmente inserir uma marca de água na imagem final adquirida pelo utilizador, para controlar a sua utilização em situações não previstas.

3.4 O sistema global do OCCAMM

O projecto OCCAMM veio proporcionar um novo mecanismo para venda e distribuição de conteúdos em formato digital aos consumidores finais, combinando a recente tecnologia de distribuição digital com os desenvolvimentos na distribuição de informação na Internet, comércio electrónico e gestão de propriedade intelectual (DRM). O sistema global do OCCAMM é composto pelos seguintes componentes [OCOOSS01]:

- Um *site* de Web (ECP – *Electronic Commerce Platform* (Plataforma de Comércio Electrónico)) na qual as encomendas de conteúdos multimédia podem ser realizadas. Contém um catálogo completo de todos os produtos para venda e permite que os utilizadores, devidamente registados, possam seleccionar os produtos para distribuição e autorizar os respectivos pagamentos. Os pagamentos podem ser efectuados de diversas formas incluindo pagamentos com cartões de crédito, pagamento por subscrição, micro pagamentos ou pagamento por utilização (*pay per use*).

- Um Servidor Multimédia, que contém todo o conteúdo disponível através do OCCAMM em formato digital. Este servidor contém o *software* responsável pela distribuição do conteúdo aos utilizadores. Este servidor está localizado na estação terrestre do fornecedor do serviço de satélite. Isto elimina a necessidade da existência de uma ligação com grande largura de banda entre este servidor multimédia e a estação de satélite terrestre por forma distribuir os produtos a pedido do utilizador final. Ao invés, o servidor está instalado na rede interna da estação de satélite terrestre, permitindo a entrega rápida e económica dos produtos solicitados através da ligação de satélite. O software de difusão é igualmente colocado no servidor multimédia, fornecendo serviços aos utilizadores. No entanto, os serviços proporcionados pelo OCCAMM não estão limitados à distribuição por satélite. Outros serviços de distribuição podem ser igualmente utilizados como por exemplo: ADSL, cabo, ligações *dial-up*, entre outras.

- O PC cliente dos utilizadores que desejam utilizar o serviço OCCAMM possui um terminal onde são capazes de efectuar a encomenda, gestão, recepção e consumo de conteúdo digital, que se encontra disponível através do sistema OCCAMM. Cada terminal de consumo necessita de possuir *hardware* e *software* capaz de realizar as funções acima citadas. A OVM é o componente principal deste terminal no PC do cliente.

- Os sistemas IPMP permitem que o conteúdo disponibilizado e distribuído através do sistema OCCAMM se encontre encriptado e sujeito a um determinado sistema IPMP. O sistema IPMP é composto por dois componentes: um cliente e outro servidor. O servidor (Sistema IPMP Servidor de Licenças) é responsável pela criação, gestão e distribuição de licenças ao PC do cliente. O cliente

(Sistema IPMP Cliente) reside no PC do cliente e comunica com o servidor através da OVM. Todas estas comunicações são protegidas pelo SAC.

- Estação de produção, que consiste numa série de ferramentas que, preparam o conteúdo para distribuição e utilização. Estas ferramentas incluem um introdutor de marcas de água, um sistema de encriptação e um codificador do formato do conteúdo (no caso do OCCAMM, o codificador é MPEG-4). Todo o conteúdo preparado pela estação de produção é transferido para o servidor multimédia para posterior distribuição aos utilizadores.

- Processador de pagamentos, capaz de proporcionar ao sistema OCCAMM uma forma de processar pagamentos para o conteúdo adquirido pelos utilizadores. Para o projecto OCCAMM o processador de pagamentos é composto por uma instituição financeira/bancária que fornece serviços de Comércio Electrónico, uma *Trusted Third Party* (TTP) proporcionando serviços de pagamento ou um sistema de micro pagamentos capazes de efectuar transacções de baixo valor. Qualquer comunicação entre a Plataforma de Comércio Electrónico e o Processador de pagamentos é segura através de uma ligação SSL/TLS, assegurando que qualquer informação financeira transferida entre duas entidades seja segura.

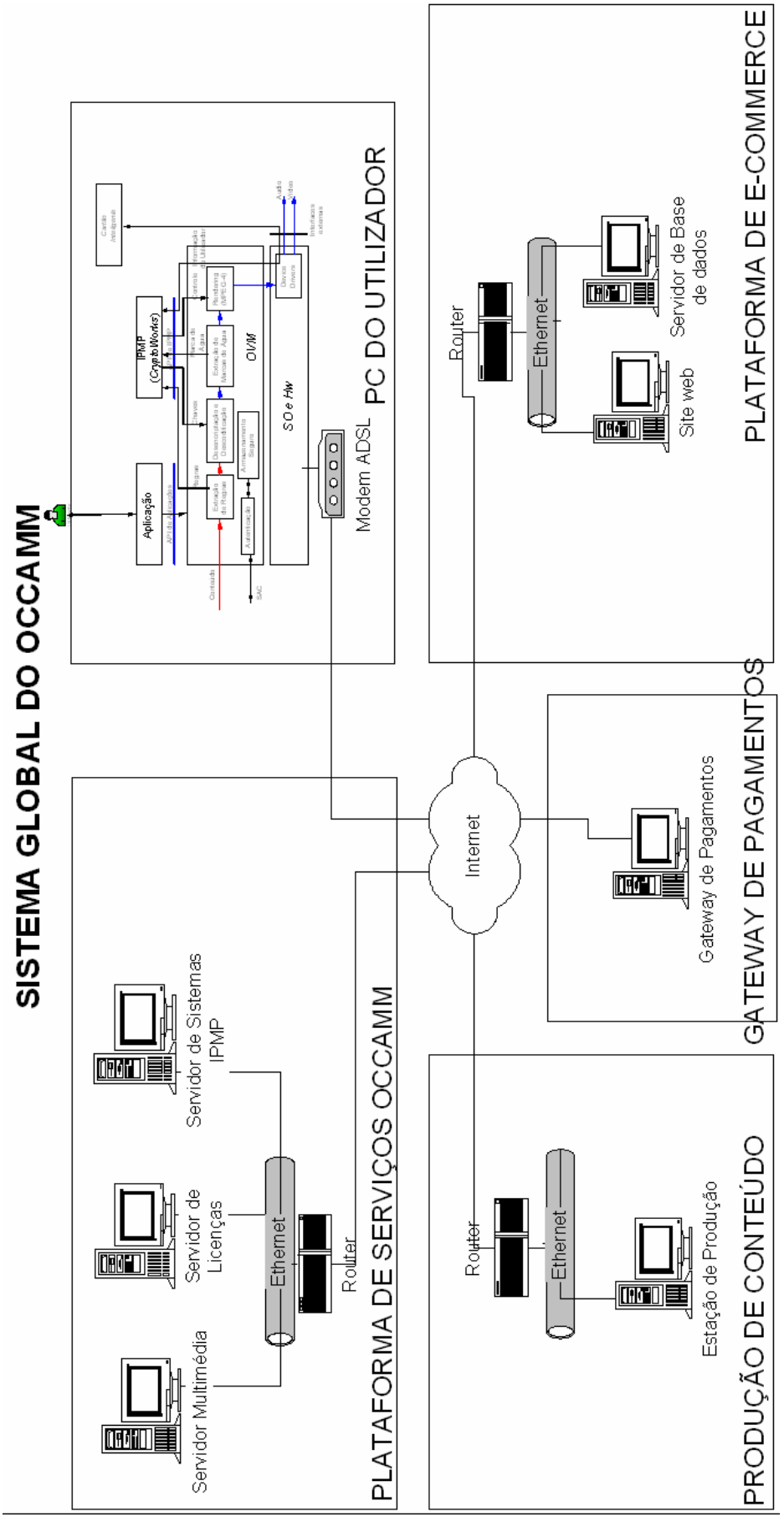


Figura 3.4 Arquitectura do sistema OCCAMM

Nesta arquitectura global (Figura 3.4), a OVM está instalada e em execução no computador pessoal do utilizador. A OVM após receber o conteúdo protegido poderá efectuar o descarregamento do sistema IPMP instalando-o e executando-o para que este controle o acesso da OVM (Figura 3.5) ao conteúdo [OCOOSSO1, OCOLSMD00].

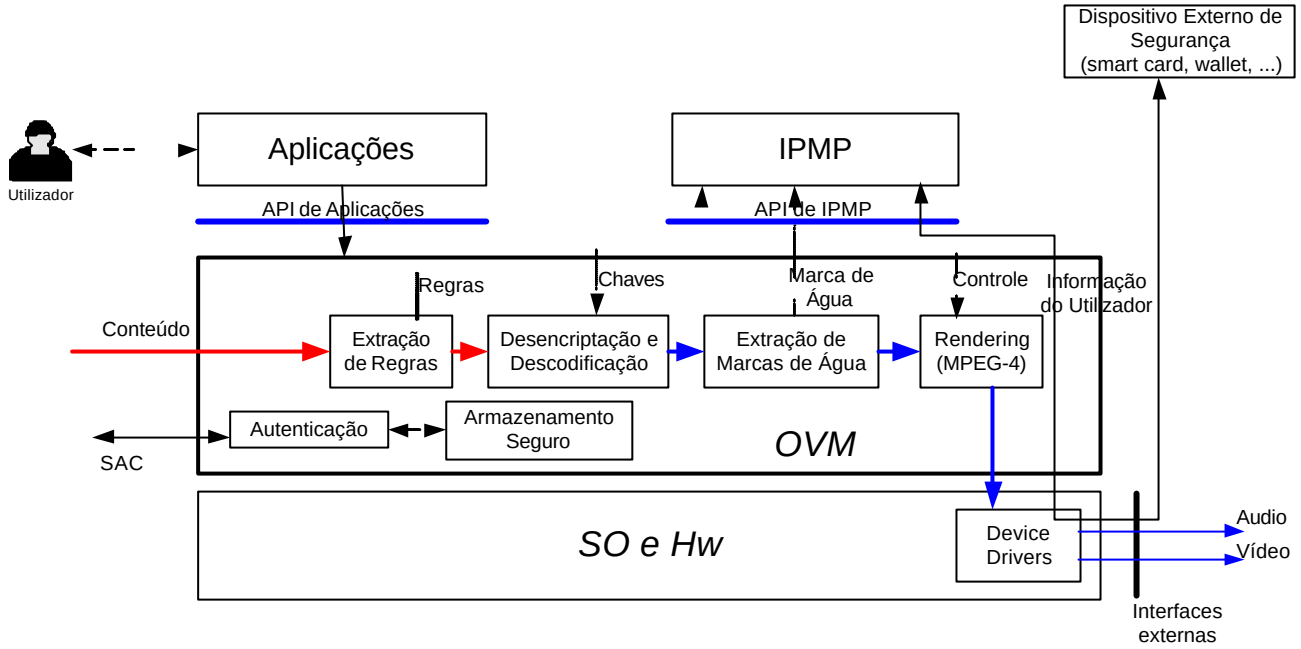


Figura 3.5 A arquitectura da OVM em detalhe

Todos os testes realizados com utilizadores do OCCAMM utilizaram a arquitectura genérica apresentada acima. Os utilizadores podem navegar num *site* de Comércio Electrónico utilizando uma ligação normal à Internet e a distribuição do conteúdo escolhido pelo cliente é realizado recorrendo a ligações de banda larga (por exemplo, via ADSL), proporcionando uma ligação rápida e fiável para a entrega do conteúdo digital [OCOLSMD00].

Um determinado utilizador que deseje adquirir produtos através do serviço OCCAMM irá utilizar sistema da seguinte forma:

- Inicialmente, o consumidor acede ao *site* de Web do OCCAMM onde pode obter conteúdo;
- O utilizador regista-se na Plataforma de Comércio Electrónico;
- O utilizador efectua a sua autenticação no *site* de Web do OCCAMM e é-lhe dada a oportunidade de utilizar uma variedade de conteúdos;
- Pode, igualmente, apenas navegar no *site* de Web como convidado, com um número de funcionalidades disponível bastante reduzido;
- Os conteúdos podem ser seleccionados para aquisição e são adicionados ao cabaz de compras. Para cada conteúdo o utilizador deve escolher a forma de utilização do mesmo;
- No fim das compras é efectuado o pagamento, através de um dos métodos de pagamento disponíveis;

- A entrega dos conteúdos é realizada após a confirmação do pagamento;
- O utilizador, para aceder a um determinado conteúdo protegido, pressiona um determinado botão; a aplicação solicita a activação de uma funcionalidade da API de Serviços de Aplicação;
- A OVM estabelece um SAC com outro OPIMA *peer* (o servidor de sistemas IPMP);
- Através do SAC, o sistema IPMP correspondente ao conteúdo seleccionado é descarregado e executado na OVM;
- O utilizador tenta abrir o conteúdo com a aplicação apropriada (neste caso um *player* de MPEG-4);
- A OVM extrai as regras de conteúdo associadas;
- O sistema IPMP analisa as regras de conteúdo;
- Se necessário o sistema IPMP descarrega do Servidor de Licenças as regras de utilização do conteúdo para o utilizador;
- Assumindo que tudo está correcto e que o utilizador possui as credenciais necessárias para a visualização do conteúdo, o sistema IPMP instrui a OVM para desencriptar e descodificar o conteúdo.
- A OVM, no caso de ser solicitado, poderá extrair a marca de água do conteúdo;
- A informação dessa marca de água é entregue ao sistema de IPMP para avaliação;
- Assumindo que a avaliação é positiva, o sistema de IPMP irá instruir a OVM para apresentar o conteúdo (*rendering*).

Neste capítulo foi descrita uma das iniciativas lançadas para lidar com a complexidade da protecção dos direitos de autor de conteúdos digitais. Esta iniciativa, designada OPIMA, especificou uma plataforma de consumo de conteúdos em segurança (OVM) assim como as interfaces de comunicação dessa plataforma com o exterior (através das APIs de Aplicações e de Sistema IPMP). A iniciativa OPIMA apenas definia estas interfaces de comunicação com componentes exteriores, não fornecendo quaisquer indicações no que diz respeito à implementação e funcionamento dos mesmos ou da própria OVM.

Com o intuito de criar a primeira implementação de uma plataforma OPIMA, surgiu o projecto OCCAMM. Este projecto levou a cabo a implementação dos seguintes componentes:

- OVM;

- Aplicação *Player* de conteúdo MPEG-4 (a funcionar sobre a OVM);

- Sistema IPMP baseado em cartões inteligentes (a funcionar sobre a OVM);

- *Site* de Comércio Electrónico para comercialização de conteúdo e Servidor de Conteúdo;

- Produção de conteúdo MPEG-4 protegido;

- Servidor de Licenças e de Sistemas IPMP.

Em suma, para além de implementar uma plataforma cliente de consumo de conteúdo seguro baseado na iniciativa OPIMA, o OCCAMM acabou por desenhar e desenvolver toda uma infra-estrutura de suporte ao comércio electrónico seguro de conteúdo digital (DRM).

No entanto, nem o OPIMA nem o OCCAMM avançaram muito no desenvolvimento de uma infra-estrutura de segurança de suporte (PKI), que permitisse que todos os componentes desenvolvidos pudessem efectuar transacções em segurança entre si. Para além disso, o sistema IPMP desenvolvido era demasiadamente específico e proprietário, com dificuldades de utilização pela maior parte dos utilizadores (inexistência de um leitor de cartões inteligentes). O sistema de pagamentos electrónicos nunca foi igualmente desenhado ou implementado. Por todos estes motivos, o sistema OCCAMM ainda estava longe de ser uma solução real para o comércio electrónico seguro de conteúdos digitais.

O próximo capítulo apresenta um sistema IPMP alternativo ao existente, baseado em *Wallets*, e define uma série de novos componentes que permitem acrescentar as funcionalidades PKI ao sistema OCCAMM. Este sistema misto DRM/PKI, apresenta algumas soluções para os problemas que foram identificados acima, quer ao nível da segurança e do controlo dos respectivos direitos de autor dos conteúdos, quer na garantia dos princípios básicos PKI (Confidencialidade, Autenticação, Integridade e Não-Repúdio) a todas as entidades do sistema.

4 APLICAÇÃO DE UMA PKI AO SISTEMA OCCAMM

4.1 Introdução

Este capítulo apresenta a especificação de um sistema IPMP alternativo e de uma plataforma genérica que é um misto de PKI com funcionalidades de DRM que se designa por OpenSDRM - *Open Secure Digital Rights Management*.

Conforme foi apresentado no capítulo anterior (Capítulo 3), quer a iniciativa OCCAMM, quer o projecto OCCAMM, não desenvolveram uma infra-estrutura de segurança de suporte (PKI) para a realização de transacções em segurança dos diferentes componentes. Assim, não era possível o estabelecimento de relações de confiança entre os diversos componentes do sistema, nomeadamente:

- Entre OVMs;
- Entre os IPMPs;
- Entre as OVMs e os IPMPs;
- Entre as OVMs e os Servidores de IPMPs;
- Entre os IPMPs e os Servidores de Licenças;
- Entre os utilizadores e a FIP;
- Entre os utilizadores e as ECP;
- Entre as ECP e as FIP;
- Entre as CAPs.

O sistema IPMP desenvolvido no âmbito do OCCAMM era igualmente proprietário e baseado em cartões inteligentes. Isto limitava a utilização do mesmo a clientes que possuíssem no seu sistema um leitor de cartões inteligentes.

De igual forma, apesar do OCCAMM ter estabelecido um teste de consumo seguro de conteúdo e de ter desenvolvido a infra-estrutura de Comércio Electrónico necessária para o comércio dos mesmos, nada especificou e desenvolveu no que respeita a pagamentos electrónicos.

Os aspectos citados acima foram a motivação para a implementação de um novo sistema IPMP incorporado numa arquitectura global de segurança e de protecção dos direitos de autor, por oposição à solução que anteriormente existia. Este é o objectivo deste capítulo, cujo conteúdo, desenvolvido e apresentado no âmbito desta dissertação, se apresenta de seguida.

De seguida é apresentada esta arquitectura global, assim como é realizada de uma forma exaustiva uma descrição de todo o protocolo do sistema OpenSDRM, com uma ênfase especial nos aspectos de segurança e no estabelecimento da confiança entre as entidades que compõem o sistema.

Por último é apresentado o modelo de PKI utilizado pelo sistema proposto neste capítulo.

4.2 O Sistema OpenSDRM

Para garantir a protecção do conteúdo digital ao nível da utilização da plataforma cliente de consumo foi necessário a utilização de um sistema IPMP. O sistema IPMP que foi desenvolvido e utilizado pelo projecto OCCAMM (conforme foi apresentado no capítulo anterior) era baseado na utilização de cartões inteligentes e num sistema de segurança proprietário da *Philips Research Laboratories* (designado por *CryptoWorks*) [OCISAFD00].

Para além do facto do sistema ser proprietário, não tinha em consideração aspectos como a integração numa solução global de protecção de conteúdo e de gestão de direitos de autor de forma a proporcionar o comércio electrónico seguro de conteúdos digitais.

O sistema aqui descrito foi implementado no âmbito da presente dissertação de Mestrado (Anexo H) e incorporando não apenas uma ferramenta IPMP para controlar o consumo do conteúdo na plataforma do cliente, como um sistema de gestão de direitos de autor e uma PKI, designado por OpenSDRM. Como já foi referido, é um sistema totalmente baseado em componentes de *software*, embora alguns destes componentes possam ser igualmente substituídos por cartões inteligentes. Um dos factores fundamentais que levou à opção pela utilização apenas de componentes de *software* prende-se com o facto da utilização de leitores de cartões inteligentes ainda não se encontrar muito difundida junto dos utilizadores de computadores pessoais (embora surjam já no mercado alguns *notebooks* equipados com leitor de cartões inteligentes), o principal público alvo dos testes de utilização real que se pretendiam realizar. O sistema OpenSDRM é mais que um simples componente de *software* que é instalado numa OVM. É acima de tudo uma infra-estrutura de confiança, baseada em PKI e composta por uma série de plataformas de *software* e *hardware* distribuídas com funcionalidades distintas, com especial incidência na protecção e gestão dos Direitos de Autor.

O sistema OpenSDRM estende o conceito do sistema IPMP tradicional definido na OPIMA e para além de desempenhar as funções de controlo de acesso ao conteúdo, funciona igualmente como um meio de pagamento electrónico. Para além disso, incorpora toda uma infra-estrutura que disponibiliza um conjunto de funcionalidades de DRM e de PKI e que oferece uma solução global para o comércio de conteúdos digitais, indo de encontro a alguns dos requisitos identificados na primeira parte da dissertação (Capítulo 1).

A arquitectura concebida para o sistema OpenSDRM é apresentada a seguir e conta com os seguintes componentes principais (Figura 4.1 e Figura 4.2):

CAP - Plataforma da Autoridade de Certificação (*Certification Authority Platform*);

ECP – Plataforma de Comércio Electrónico (*Electronic Commerce Platform*);

FIP – Plataforma da Instituição Financeira (*Financial Institution Platform*);

UCP – Plataforma de Consumo do Utilizador (*User Consumer Platform*).

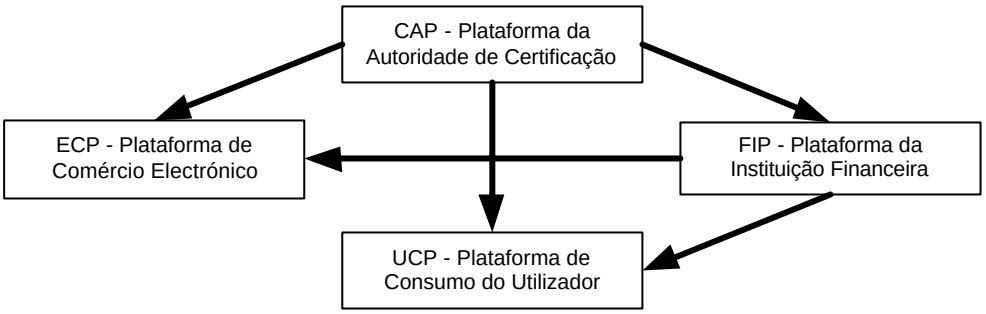


Figura 4.1 Arquitectura geral do sistema

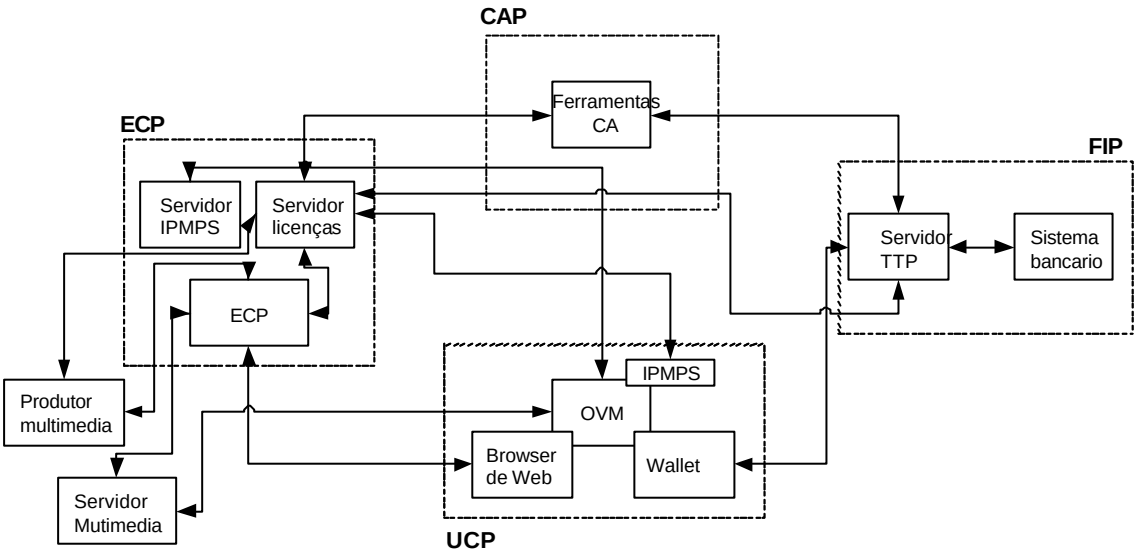


Figura 4.2 Relações entre as entidades do sistema OpenSDRM

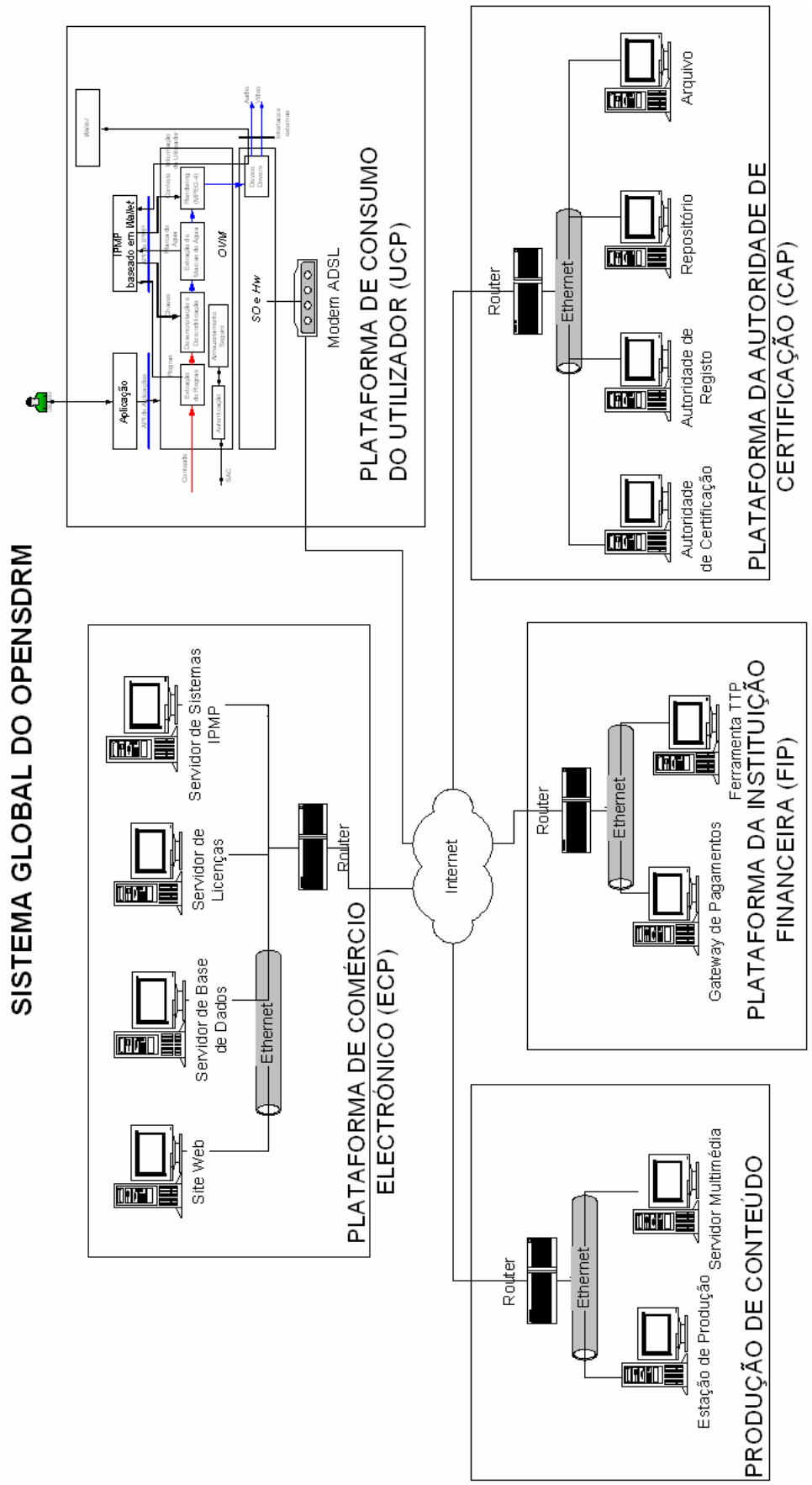


Figura 4.3 Arquitectura detalhada do Sistema OpenSDRM

Na arquitectura acima apresentada (Figura 4.3), cada um dos blocos indica as entidades, enquanto que as setas indicam o estabelecimento de mecanismos de confiança entre essas mesmas entidades. Existem algumas entidades (ECP, UCP e FIP) que recebem da CAP dois mecanismos de confiança distintos (credenciais) (Figura 4.4): um baseado em X.509 e outro baseado em XML. O sistema OpenSDRM ao utilizar estes dois mecanismos acaba por suportar dois níveis de segurança distintos: um primeiro nível designado por nível de transporte (baseado em X.509) e um segundo nível designado por nível transaccional (baseado em XML) (Figura 4.4). Estes dois níveis distintos de segurança permitem o estabelecimento das necessárias e adequadas relações de confiança entre as diferentes entidades do sistema, assim como levantam dificuldades acrescidas a entidades externas ao sistema que tentem quebrá-lo.

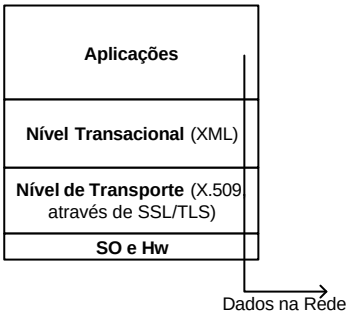


Figura 4.4 Níveis de Segurança

- Nível de Transporte: este nível de segurança é utilizado para manter o canal de comunicações seguro e autenticado, baseado em tecnologia perfeitamente normalizada, usando o protocolo SSL/TLS e os certificados X.509 para esta tarefa. Apesar de seguro, este nível apenas garante a autenticação bidireccional das entidades em comunicação (computadores), não garantindo a autenticação dos utilizadores particulares nem das transacções realizadas entre eles. Este nível é perfeitamente independente das aplicações que o utilizam;

- Nível Transaccional: este nível de segurança utiliza o nível de transporte que foi especificado acima, sendo baseado em XML. Este nível permite garantir a segurança e autenticação das transacções realizadas entre as diversas aplicações. Este nível é dependente das aplicações que o utilizam e deve obedecer a protocolos e notações previamente especificados, que podem ser proprietários;

Nas próximas secções apresentam-se os diferentes componentes da arquitectura, os seus detalhes e uma descrição do protocolo de comunicação utilizado pelos mesmos.

4.2.1 CAP - Plataforma da Autoridade de Certificação

No sistema apresentado, a CAP, ou Plataforma da Autoridade de Certificação (Figura 4.5), é a entidade responsável pela emissão das credenciais de segurança dos dois níveis citados acima: (a) emissão de credenciais em formato X.509 necessários para a credenciação da OVM e estabelecimento do SAC e (b) emissão de credenciais em formato XML necessárias para a certificação das mensagens trocadas entre as diversas entidades. As assinaturas digitais colocadas nas credenciais XML seguem a norma W3C XMLDSig (ver capítulo 2).

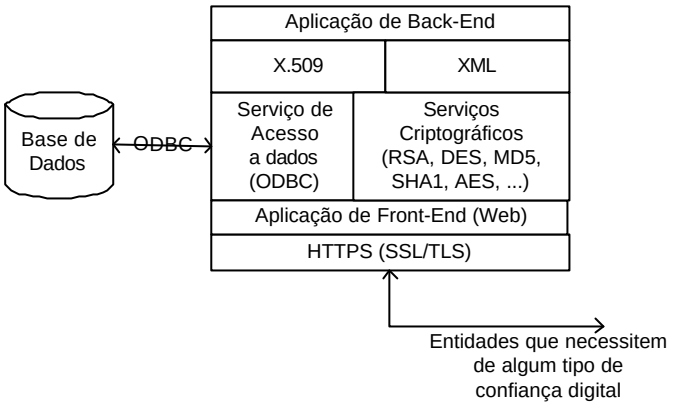


Figura 4.5 Arquitectura Técnica da Ferramenta de Certificação

A CAP permite garantir confiança às restantes entidades do sistema. As entidades que necessitem de efectuar o estabelecimento de relações de confiança entre si recorrem ao sistema de certificação de forma a obter uma credencial apropriada para a finalidade requerida. A CAP emite credenciais para as diversas OVM (tal como a norma OPIMA especifica), permitindo que estas possam estabelecer o SAC entre si e com outras entidades externas. Permite igualmente a emissão de credenciais para garantir a segurança transaccional do sistema.

Este sistema de emissão de credenciais possui alguns elementos importantes, nomeadamente uma aplicação de *front-end* desenvolvida em ambiente Web e uma aplicação de *back-end*. A aplicação de *front-end* interage com as entidades que solicitam credenciais na plataforma de certificação, enquanto que a aplicação de *back-end* interage directamente com o administrador da plataforma de certificação responsável pela emissão das mesmas.

Entre as funcionalidades da CAP destacam-se algumas pela sua importância:

- Recepção de pedidos de emissão de certificados em formato X.509 pelas diversas entidades;
- Recepção de pedidos de emissão de certificados em formato XML pelas diversas entidades;
- Emissão de certificados em formato X.509 (para certificar OVMs e o código descarregável do sistema IPMP, e ainda para o estabelecimento das ligações SSL/TLS entre as diversas entidades da arquitectura OpenSDRM);
- Emissão de certificados XML (para certificar as transacções entre as diversas entidades da arquitectura OpenSDRM)
- Gestão da emissão dos certificados e verificação dos dados contidos nos mesmos.

O seguinte diagrama de *Use-Case* (utilizando a linguagem de modelação visual UML[38]), especifica todas as funcionalidades desta CAP (Figura 4.6) assim como as interacções desta com actores externos.

[38] *Unified Modelling Language*

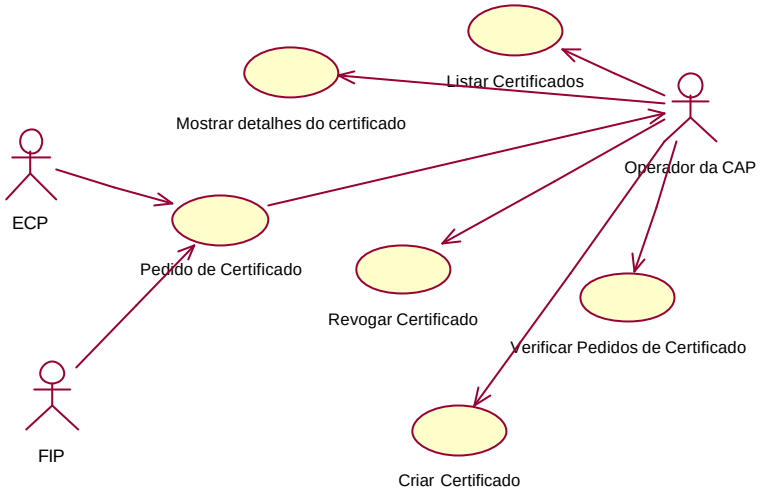


Figura 4.6 Diagrama de Use Case da CAP

4.2.2 ECP – Plataforma de Comércio Electrónico

A Plataforma de Comércio Electrónico é responsável pela implementação dos mecanismos necessários para a viabilização da comercialização electrónica dos bens e serviços assim como dos mecanismos de confiança necessários entre a loja virtual e o utilizador final (Figura 4.7).

Os mecanismos de segurança/confiança proporcionados pela ECP são o servidor de módulos IPMP e o servidor de licenças. Em conjunto, permitem assegurar que o conteúdo adquirido nesta plataforma de comércio electrónico seja utilizado de acordo com as regras que foram negociadas e definidas aquando da aquisição do mesmo.

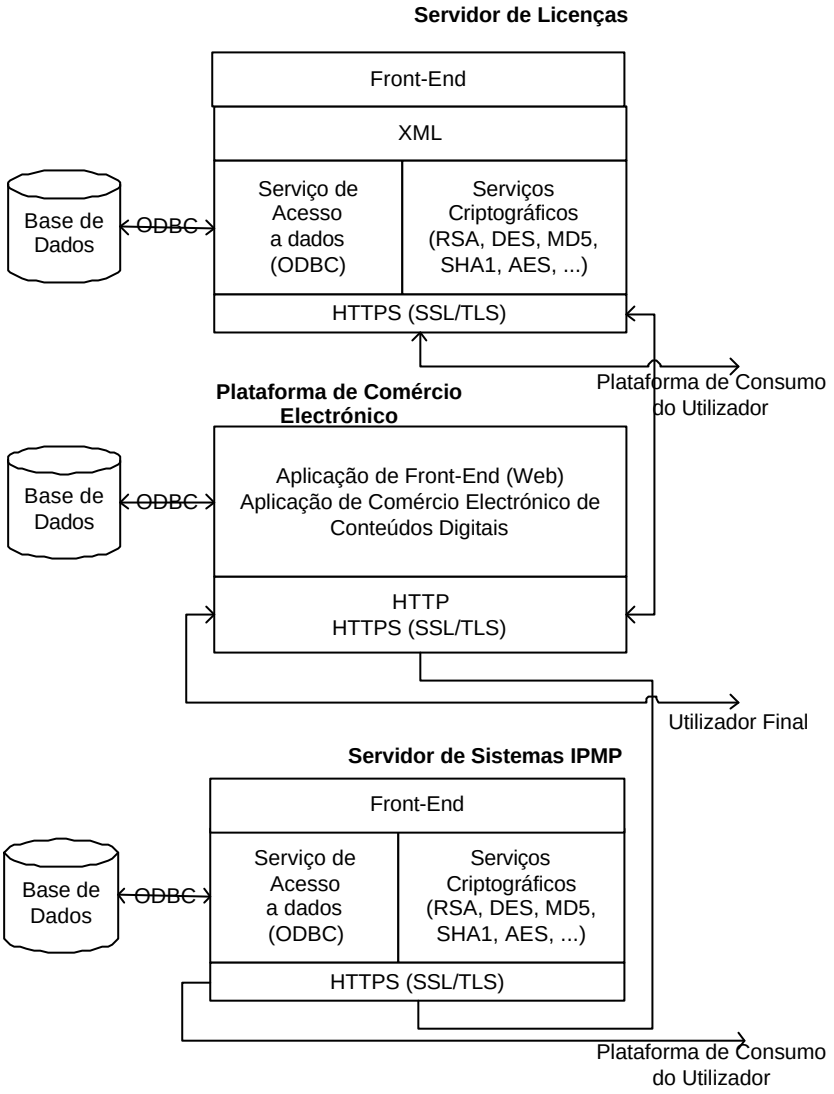


Figura 4.7 Arquitectura Técnica da Plataforma de Comércio Electrónico

Algumas das funcionalidades mais importantes da ECP são:

- A operação da Plataforma de Comércio Electrónico (comercialização do conteúdo, gestão de utilizadores, gestão do conteúdo, descarregamento de conteúdo digital protegido);
- A criação de licenças para a utilização de conteúdo adquirido, de acordo com a negociação interactiva com o utilizador;
- O fornecimento seguro de licenças por parte do sistema OpenSDRM;
- A gestão de licenças e de dados de pagamento;
- A gestão de sistemas IPMP;
- O fornecimento seguro de sistemas IPMP.

O seguinte diagrama de *Use-Case* (Figura 4.8), especifica todas as funcionalidades desta Plataforma de Comércio Electrónico assim como as interacções desta com actores externos.

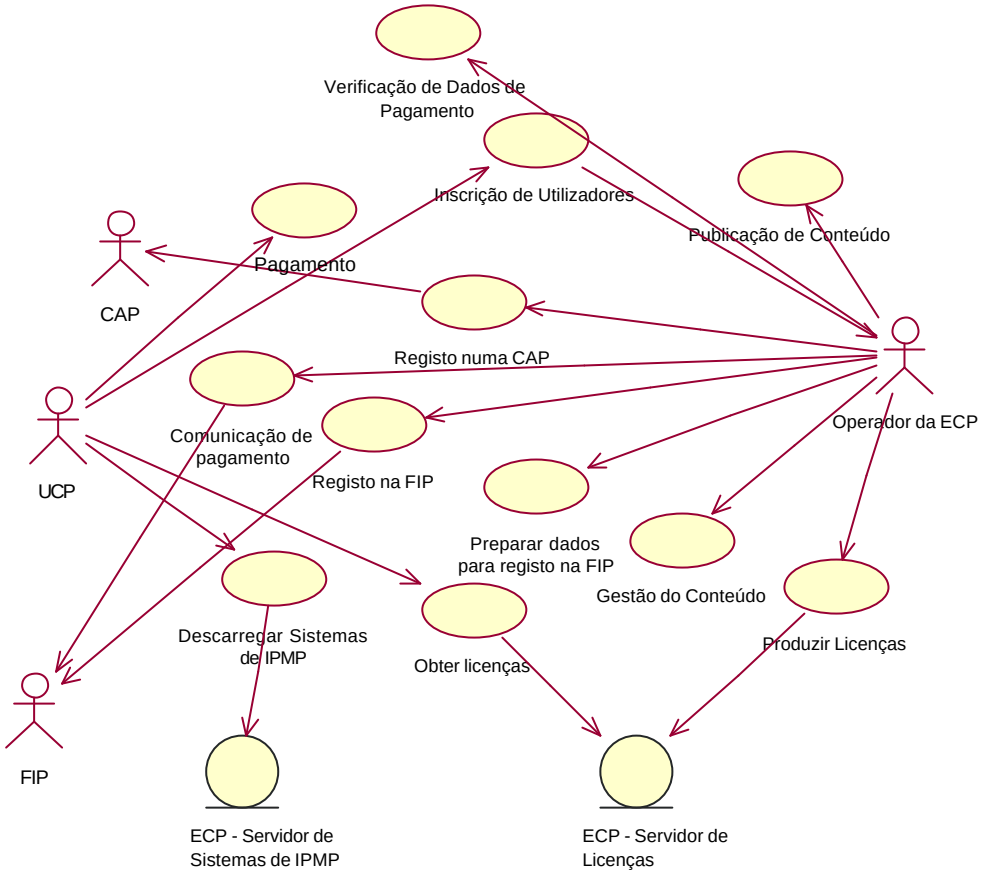


Figura 4.8 Diagrama de Use Case da ECP

4.2.3 FIP – Plataforma da Instituição Financeira

A Plataforma da Instituição Financeira corresponde ao ponto de ligação entre o sistema OpenSDRM e o sistema financeiro de pagamentos reais (rede financeira). A ligação para este sistema financeiro é garantida através de uma ferramenta designada por TTP – *Trusted Third Party* (Figura 4.9). Esta ferramenta é responsável pela emissão das credenciais necessárias para os utilizadores e para a(s) Plataforma(s) de Comércio Electrónico, permitindo o estabelecimento da confiança transaccional entre ambos. As credenciais emitidas por esta ferramenta estão codificadas em formato XML (o formato das assinaturas digitais utiliza a norma W3C XMLDSig (ver secção 2.7.2) [EXMLS01]).

Este sistema não é dependente de qualquer forma específica de pagamento, podendo ser utilizado em conjunto com qualquer forma de pagamento. No entanto, não faz parte do âmbito do OpenSDRM a especificação do sistema a montante da instituição financeira, assim como da definição das trocas de informação entre as diversas instituições financeiras.

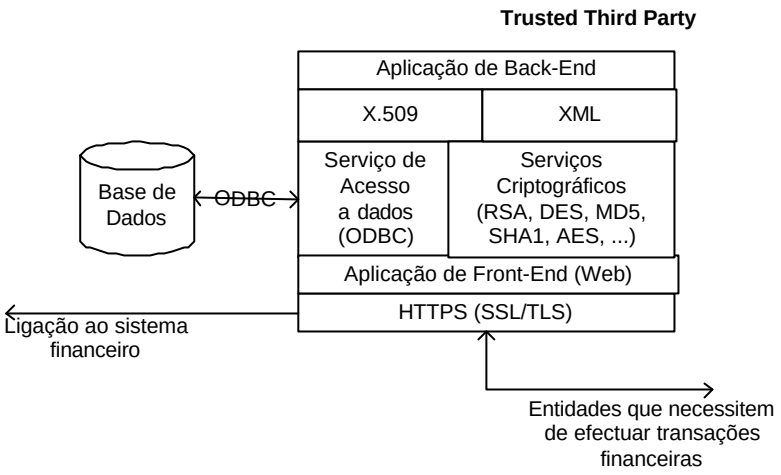


Figura 4.9 Arquitectura Técnica da Plataforma da Instituição Financeira

Algumas das funcionalidades mais importantes da FIP são:

- A recepção de pedidos para a emissão de credenciais transaccionais em formato XML para Plataformas de Comércio Electrónico (por exemplo, com dados financeiros relativos ao número da conta bancária da Plataforma de Comércio Electrónico);
- A recepção de pedidos para a emissão de credenciais transaccionais em formato XML para utilizadores (por exemplo, com dados financeiros relativos ao número de cartão de crédito do utilizador);
- A emissão de credenciais transaccionais em formato XML para Plataformas de Comércio Electrónico;
- A emissão de credenciais transaccionais em formato XML para utilizadores;
- O processamento das ordens de pagamento enviadas por parte de ECPs que foram emitidas por utilizadores;

O seguinte diagrama de *Use-Case* (Figura 4.10) especifica todas as funcionalidades desta Plataforma da Instituição Financeira assim como as interacções desta com actores externos.

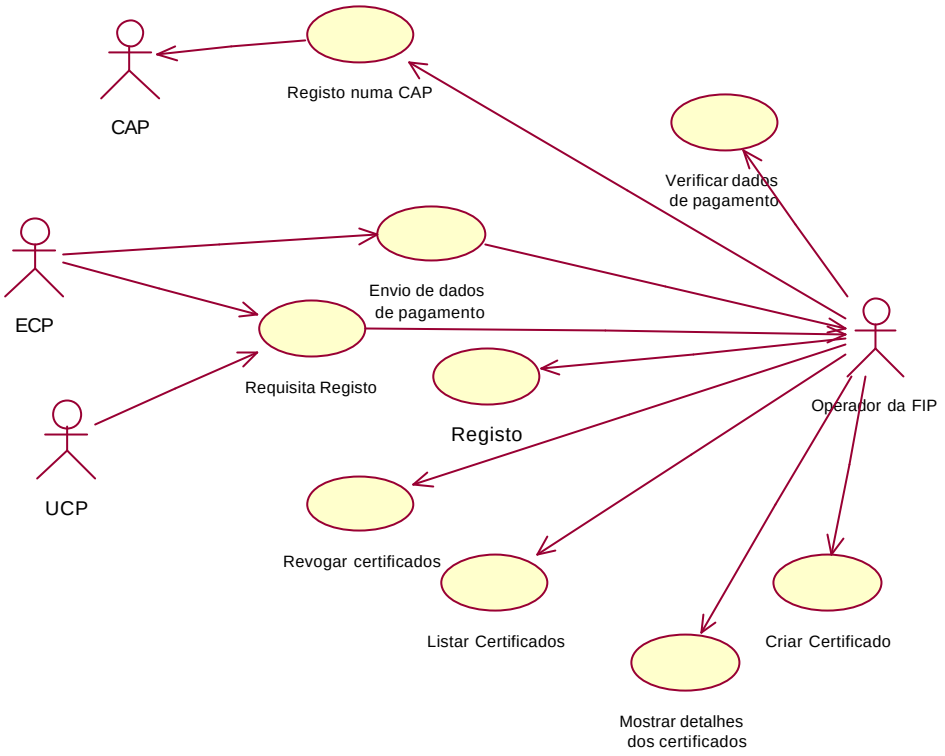


Figura 4.10 Diagrama de Use Case da FIP

4.2.4 UCP – Plataforma de Consumo do Utilizador

A Plataforma de Consumo do Utilizador é composta pelo conjunto de componentes de *software* que permitem ao utilizador aceder e utilizar conteúdos multimédia de uma forma segura e com a respectiva salvaguarda dos direitos de autor desses mesmos conteúdos. Para além disso, o sistema OpenSDRM permite ainda garantir que o consumidor efectuará o pagamento dos conteúdos que utilizar. Os componentes que compõem esta plataforma são os seguintes:

- *Browser* de Web: utilizado para navegar na WWW e efectuar a escolha do conteúdo multimédia que se deseja consumir assim como para negociar as condições de utilização do mesmo;
- OVM: utilizado para consumir conteúdo multimédia seguro de acordo com as regras de utilização previamente estabelecidas;
- Sistema IPMP baseado em *Wallet*: funciona sobre a OVM e faz com que o utilizador possa utilizar o conteúdo e que este seja usado de acordo com regras estabelecidas;
- *Wallet*: componente de *software* que contém os dados de segurança do utilizador. Os dados de segurança são armazenados na *Wallet* num repositório seguro e encriptado, usando PKCS#5 (ver Anexo F, Tabela F.6), que apenas pode ser acedido com a chave correcta (nome de utilizador e palavra-chave);

As funcionalidades principais da UCP são as seguintes:

- Navegar no conteúdo multimédia disponível na Plataforma de Comércio Electrónico utilizando um *browser* Web;
- Descarregar conteúdo multimédia da plataforma de comércio electrónico para a UCP;
- Negociar as condições de utilização dos conteúdos multimédia;
- Consumir conteúdo multimédia de forma segura;
- Descarregar os sistemas IPMP dos servidores de sistemas IPMP e instalá-los na UCP;
- Descarregar as licenças do servidor de licenças.

O seguinte diagrama de *Use-Case* (Figura 4.11), especifica todas as funcionalidades desta Plataforma de Consumo do Utilizador assim como as interacções desta com actores externos.

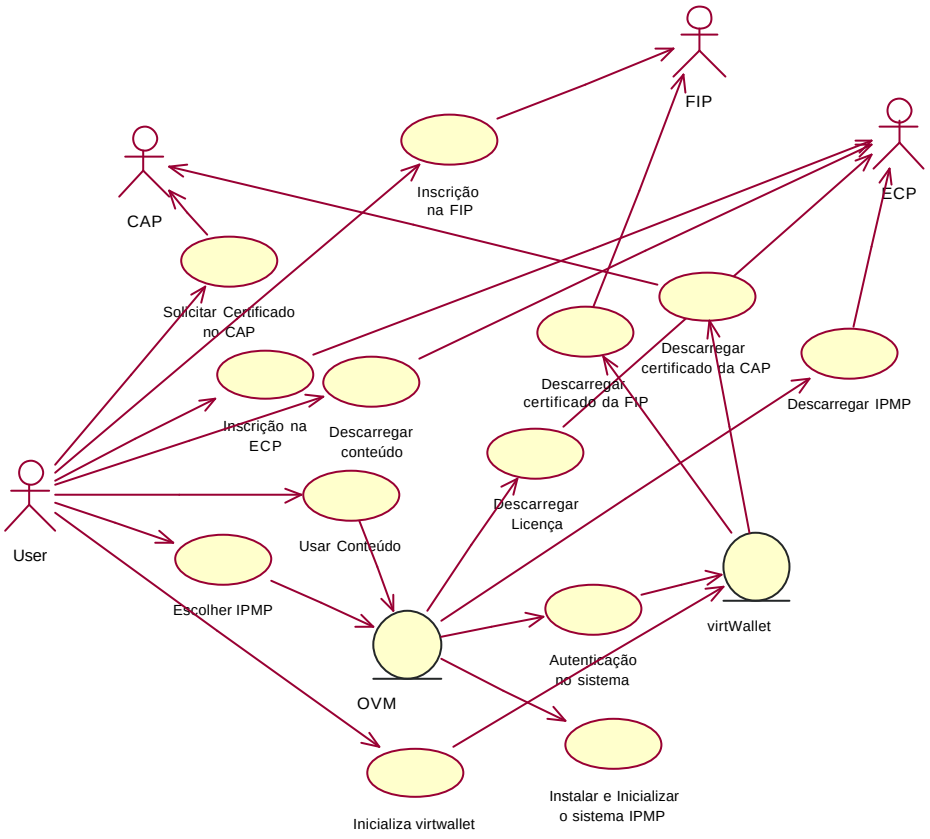


Figura 4.11 Diagrama de Use Case da UCP

4.2.5 Descrição funcional do sistema (descritivo)

Esta secção descreve o funcionamento do sistema OpenSDRM, desde as normais operações de inicialização do sistema até ao consumo do conteúdo digital multimédia.

Inicialmente, todos os elementos do sistema (ECP, FIP, UCP) precisam de estar devidamente certificados pela Plataforma da Autoridade de Certificação. Aliás a própria CAP precisa de estar devidamente certificada de forma a inicializar todo o sistema de segurança/confiança. Esta certificação pode ser realizada usando uma das seguintes formas: (1) a CAP pode obter um certificado digital a partir de uma autoridade de certificação já existente no mercado (*Verisign*[39], *Thawte*[40], *Certipor*[41] ou qualquer outra), significando que a confiança do sistema é estabelecida a partir de uma entidade externa, ou então, (2) a CAP gera o seu próprio certificado digital (auto-certificação), em que o sistema de confiança depende única e exclusivamente da CAP (sendo este o ponto base de confiança da cadeia de certificados). Assim, a CAP recorrendo a um algoritmo de criptografia de chave assimétrica (RSA), gera um par de chaves, uma pública e outra privada ($Kpub^{CAP}$, $Kpriv^{CAP}$), e solicita um certificado digital a uma autoridade de certificação externa ao sistema ($Cert_{AutExt}{}^{X509}\{K_{pub}{}^{CAP}\}$). Em alternativa pode gerar o seu próprio certificado digital ($Cert_{CAP}{}^{X509}\{Kpub^{CAP}\}$). Ambos permitem garantir a autenticidade desta entidade. A CAP emite igualmente um certificado para si própria em formato XML ($Cert_{CAP}{}^{XML}\{K_{pub}{}^{CAP}\}$). Este certificado irá estabelecer a base de confiança de todo o sistema transaccional. A $Kpriv^{CAP}$ deve estar armazenada num dispositivo seguro, de forma a evitar que esta possa ser roubada e utilizada indevidamente por terceiros para gerar certificados digitais em nome da CAP. A $Kpub^{CAP}$ pode ser disponibilizada para todas as entidades do sistema (sob a forma de um certificado digital ($Cert_{CAP}{}^{XML}\{Kpub^{CAP}\}$)), pois irá ser utilizada para verificar os certificados digitais que forem emitidos pela CAP.

A Plataforma de Comércio Electrónico gera igualmente um par de chaves criptográficas, uma pública e outra privada ($Kpub^{ECP}$, $Kpriv^{ECP}$). A chave privada é mantida confidencial, enquanto que a correspondente chave pública é submetida à CAP para que esta seja certificada digitalmente. Assim, a ECP submete $Kpub^{ECP}$ juntamente com informação pessoal e a CAP emite um certificado digital em que comprova a identidade real e digital da ECP ($Cert_{CAP}{}^{X.509}\{Kpub^{ECP}\}$, $Cert_{CAP}{}^{XML}\{Kpub^{ECP}\}$).

O certificado $Cert_{CAP}{}^{X.509}\{Kpub^{ECP}\}$ é instalado no servidor de Web e nas aplicações que irão comunicar futuramente através de SSL/TLS, enquanto que $Cert_{CAP}{}^{XML}\{Kpub^{ECP}\}$ é instalado na Base de Dados do Servidor de Licenças.

A Plataforma da Instituição Financeira gera um par de chaves criptográficas ($Kpub^{FIP}$, $Kpriv^{FIP}$), uma pública e outra privada, em que a chave privada é mantida secreta enquanto que a pública é submetida à CAP para ser digitalmente certificada. Esta FIP obtém dois tipos de credenciais distintas: uma que será utilizada para o estabelecimento de confiança ao nível da camada de transporte, baseada em X.509, e outro utilizado para estabelecer confiança ao nível transaccional, baseado em XML. A CAP gera então um certificado digital X.509 ($Cert_{CAP}{}^{X.509}\{Kpub^{FIP}\}$) que a FIP vai utilizar para instalar no seu servidor de Web e na sua OVM para permitir ligações seguras SSL/TLS. Um outro certificado digital é gerado pela CAP e enviado para a FIP para ser instalado por esta ($Cert_{CAP}{}^{XML}\{Kpub^{FIP}\}$) por forma a garantir a segurança transaccional da FIP com as restantes entidades do sistema.

[39] http://www.verisign.com

[40] http://www.thawte.com

[41] http://www.certipor.pt

O certificado $Cert_{CAP}^{X.509}\{Kpub^{FIP}\}$ é instalado no servidor de Web e nas aplicações que vão comunicar através de SSL/TLS, enquanto que $Cert_{CAP}^{XML}\{Kpub^{FIP}\}$ é instalado na Base de Dados da *Trusted Third Party*.

A emissão destes certificados pela CAP permite que FIPs e ECPs possam estabelecer relações de confiança entre si sem que para isso tenham que se conhecer à partida. Assim, basta que ambas confiem na mesma CAP ou então em CAPs que descendam de um caminho de certificação comum para que possam estabelecer confiança entre si (ou ainda que tenham efectuado uma certificação cruzada entre si). Esta primeira certificação permite estabelecer o nível de confiança e segurança a nível das comunicações de rede.

Para que a ECP possa efectuar transacções financeiras por via dos serviços prestados (a comercialização de conteúdo multimédia) é necessário que esteja registada numa instituição financeira (ou várias). Esta instituição financeira (FIP) possui os sistemas adequados (TTP, *Gateway* de Pagamentos) que permitem a validação dos meios de pagamento apresentados pelos utilizadores. Este sistema não é dependente de nenhum meio de pagamento específico e pode ser utilizado com meios de pagamento distintos (cartão de crédito, cartão de débito, débito directo em conta, transferência bancária, entre outros). A ECP possui uma conta bancária própria associada ao sistema para que possam ser creditados os valores provenientes dos diversos utilizadores. Assim, a FIP estabelece a confiança entre ECPs e utilizadores que nunca se cruzaram. Esta garantia permite que (1) os utilizadores se assegurem que estão a enviar os seus dados para ECPs válidas e (2) às ECPs que estas irão receber as respectivas contrapartidas financeiras pelos serviços que prestam.

Para que esta confiança mútua se possa estabelecer, a ECP submete a sua chave pública, $Kpub^{ECP}$, a uma FIP, onde possui uma conta bancária em que são creditados os valores dos serviços prestados por esta. A ECP submete os seus dados, em conjunto com o certificado emitido pela CAP ($Cert_{CAP}^{XML}\{Kpub^{ECP}\}$) para a FIP. Esta regista os dados da ECP e emite um novo certificado ($Cert_{FIP}^{XML}\{Kpub^{ECP}\}$). A ECP instala este seu novo certificado no seu sistema.

Sempre que um determinado utilizador deseja aderir ao sistema OpenSDRM através da utilização de uma aplicação com uma OVM integrada numa Plataforma de Consumo de Conteúdo OPIMA/OCCAMM precisa de possuir um dispositivo em que os seus dados pessoais sejam salvaguardados: cartão inteligente ou através de uma *Wallet* baseada em *software*. Tanto o cartão inteligente como a *Wallet* armazenarão os dados públicos e privados do utilizador em segurança, nomeadamente as suas chaves criptográficas, assim como os certificados que forem obtidos de autoridades emissoras apropriadas. Como objecto da presente dissertação de Mestrado, o sistema que será analisado é o baseado numa *Wallet*. A *Wallet*, não é mais do que *software* que "replica" o funcionamento e algumas funcionalidades de um cartão inteligente, embora o nível de segurança destes dispositivos seja muito superior.

A *Wallet* utiliza um mecanismo que armazena de forma segura os dados privados do utilizador. Os dados encontram-se armazenados em segurança usando o PKCS#5 (Anexo F, Tabela F.6). O processo de registo de uma *Wallet* e consequentemente de um utilizador ou UCP encontra-se descrito nos seguintes passos:

1. Escolha de um nome de utilizador e de uma palavra-chave: o utilizador deve escolher um nome de utilizador (*login*) e a correspondente palavra-chave (*password*);

2. O software da *Wallet* gera um par de chaves criptográficas: uma pública e outra privada ($Kpub^{UCP}$, $Kpriv^{UCP}$);

3. Escolha da chave para o repositório seguro de informação na *Wallet*: utilizando como entradas o nome do utilizador e a palavra-chave escolhidas pelo utilizador, é construída uma chave criptográfica secreta para o algoritmo de encriptação (baseado em PKCS#5 (Anexo F, Tabela F.6)), ($K_{PKCS\#5}$=calculaChave(nome_utilizador, palavra_chave)). Os dados privados do utilizador ficam armazenados neste repositório de forma segura. Desta forma garante-se que apenas o detentor da informação (nome de utilizador, palavra-chave) consegue aceder a este repositório seguro e consultar os seus dados secretos;

4. Armazenamento seguro do par de chaves criptográficas geradas: utilizando a chave gerada no passo anterior as chaves criptográficas ($Kpub^{UCP}$, $Kpriv^{UCP}$) são armazenadas no repositório seguro da *Wallet* ($K_{PKCS\#5}[Kpub^{UCP}]$, $K_{PKCS\#11}[Kpriv^{UCP}]$);

5. Certificação da *Wallet*: para que a *Wallet* possa ser reconhecida como sendo parte integrante do sistema OpenSDRM é necessário que esteja registada na CAP. Assim, o utilizador regista os seus dados (nome de utilizador, palavra chave, $Kpub^{UCP}$) na CAP. É importante que o utilizador registe o seu nome de utilizador e palavra-chave, uma vez que esta é a única forma possível que o utilizador tem de recuperar a sua palavra-chave no caso de extravio da mesma;

6. Emissão da credencial da CAP: a CAP emite um certificado ($Cert_{CAP}{}^{XML}\{Kpub^{UCP}\}$) que transmite a confiança necessária a todos os dados submetidos pelo utilizador à CAP;

7. Armazenamento local do certificado da CAP: o UCP armazena o certificado obtido da CAP ($Cert_{CAP}{}^{XML}\{Kpub^{UCP}\}$) na *Wallet*, mais especificamente no seu repositório seguro de dados ($K_{PKCS\#5}[Cert_{CAP}{}^{XML}\{Kpub^{UCP}\}]$);

8. Registo da UCP numa FIP: para que a UCP possa passar a efectuar transacções financeiras com uma ECP válida deve registar-se na ECP, apresentando para isso uma credencial validada por uma FIP, atestando uma forma de pagamento válida (independente da mesma). Assim, a UCP fornece à FIP um meio de pagamento e o certificado obtido da CAP (meio de pagamento, $Cert_{CAP}{}^{XML}\{Kpub^{UCP}\}$). Este meio de pagamento será verificado e validado pela FIP e o certificado emitido pela CAP serve para garantir à FIP que se trata de uma UCP válida que obteve acesso ao sistema de uma forma válida. Tal facto permite o estabelecimento de confiança entre UCPs e FIPs que nunca se encontraram frente a frente;

9. Emissão da credencial da FIP: a FIP, após boa verificação dos dados fornecidos pela UCP, emite uma credencial ($Cert_{FIP}{}^{XML}\{Kpub^{UCP}\}$). Esta credencial vai permitir garantir a quem a receber que a UCP é válida assim como o seu meio de pagamento;

10. Armazenamento do certificado do FIP: a UCP recebe e armazena de uma forma segura o certificado obtido da FIP ($K_{PKCS\#5}[Cert_{FIP}{}^{XML}\{Kpub^{UCP}\}]$);

11. A UCP irá possuir no final de todo este processo os seguintes dados armazenados de forma segura: $K_{PKCS\#5}[Kpub^{UCP}, Kpriv^{UCP}, Cert_{CAP}{}^{XML}\{Kpub^{UCP}\}, Cert_{FIP}{}^{XML}\{Kpub^{UCP}\}]$

Para que o utilizador possa adquirir conteúdo digital na ECP precisa de estar registado na mesma. O processo de registo numa ECP tradicional baseia-se no conjunto constituído pelo nome do utilizador e pela palavra-chave que o permite autenticar-se. A confiança é estabelecida individualmente entre o utilizador e a ECP, não existindo nenhuma garantia à partida por parte da ECP de que os utilizadores são válidos, e de que o meio de pagamento fornecido por estes é de confiança. No sistema apresentado, existe uma terceira entidade (FIP), que garante à ECP que os dados fornecidos pelo utilizador são válidos e que consequentemente, o meio de pagamento apresentado também o será. Ao utilizador são apresentadas provas de confiança por parte da ECP que permitem que o utilizador possa confiar nesta. Os dados de pagamento reais nunca são directamente enviados para a ECP assim como a verdadeira identidade do utilizador não é igualmente revelada. Este facto garante um aspecto importante nas relações electrónicas: a privacidade.

Durante a inscrição na ECP, o utilizador usa as credenciais fornecidas pela FIP. A ECP verifica estas mesmas credenciais e regista o utilizador. Durante este registo é solicitado ao utilizador a introdução de uma palavra-chave que permite que este possa adquirir conteúdo digital na ECP.

Quando um utilizador registado pretende adquirir um determinado conteúdo digital numa ECP, escolhe qual o conteúdo que deseja e posteriormente negoceia os termos de utilização do mesmo. Este facto leva à correspondente produção de uma licença para o conteúdo em causa. Para que a negociação possa ser bem sucedida é necessário que o utilizador prove que está efectivamente registado na ECP, utilizando para isso o nome do utilizador e a correspondente palavra-chave configuradas no passo anterior.

O objectivo final do presente sistema consiste na protecção do conteúdo digital adquirido e na salvaguarda dos direitos de autor do mesmo. Esse conteúdo digital é adquirido numa ECP, e consumido numa plataforma cliente com uma OVM garantindo que os direitos de autor são preservados. Por outro lado, o laço de confiança existente entre o utilizador e a ECP, garantido pelas credenciais emitidas pela FIP, permite ao utilizador acreditar que a ECP fornecerá o conteúdo previamente pago. Por sua vez, estas credenciais garantem à ECP que esta receberá o pagamento pelo conteúdo fornecido ao utilizador.

Quando o utilizador adquire um conteúdo digital numa ECP são executados vários procedimentos:

1. O utilizador utiliza o *browser* de Web para navegar no *site* do ECP;

2. O utilizador escolhe conteúdo digital no ECP;

3. O utilizador negoceia as condições de licenciamento de um determinado conteúdo, e apresenta à ECP o seu nome de utilizador e palavra-chave escolhidos no processo de inscrição da mesma;

4. A ECP verifica a credencial fornecida pelo UCP e produz uma licença para o conteúdo em causa. A licença não é mais do que uma credencial gerada pela ECP que contem diversos dados representativos da mesma ($Cert_{ECP}{}^{XML}\{LIC(UCP_{id}+C_{id})\}$). O formato da licença em causa utiliza um

subconjunto bastante reduzido da norma ODRL[42]. O ODRL é uma linguagem baseada em XML utilizada para exprimir os direitos de utilização de um determinado conteúdo;

Através do sistema IPMP e da correspondente OVM, a UCP verifica a existência na plataforma de uma licença adequada para visualizar o conteúdo protegido em causa. No caso da não existência da mesma torna-se necessário proceder ao descarregamento desta a partir da ECP. A UCP envia um pedido da licença para a ECP ($REQ^{XML}\{C_{id}+UCP_{id}\}$). A ECP verifica o pedido efectuado pela UCP e, no caso do pedido estar correctamente formatado e válido, envia como resposta a licença solicitada ($Cert_{ECP}{}^{XML}\{LIC[C_{id}+UCP_{id}+UR_{play}+UR_{copies}+C_{key}+Value]\}$).

Após a recepção do certificado com a licença para o conteúdo, o sistema IPMP produz um certificado especial contendo a autorização da UCP para que a ECP possa receber o valor monetário em causa pelo serviço prestado ao utilizador. A ECP pode assim armazenar todos estes certificados e mais tarde processar todos os recebimentos, junto de uma FIP, ou processá-los de imediato *on-line*.

Os diversos procedimentos são realizados no processamento dos pagamentos:

1. UCP emite a autorização de pagamento para a ECP ($Cert_{UCP}{}^{XML}\{PAYdata[U_{id}+Value]\}$)
2. ECP recebe os dados e armazena-os para os enviar mais tarde para a FIP ($Cert_{ECP}{}^{XML}\{Cert_{UCP}{}^{XML}\{PAYdata(U_{id}+Value)\}\}$)
3. Na posse destes dados a FIP consegue validar tanto a ECP assim como a UCP, uma vez que ambas se encontram registadas numa FIP válida.

4.2.6 Descrição do protocolo do sistema (normativa)

Esta secção descreve o funcionamento e o protocolo do sistema e apresenta uma descrição de todas as mensagens que são trocadas no mesmo.

4.2.6.1 Inicialização do sistema

Ao longo desta fase são realizadas diversas inicializações que ocorrem nas várias entidades do sistema. Fundamentalmente, todas as entidades geram pares de chaves criptográficas recorrendo a um algoritmo de chave pública (neste caso o RSA).

CAP	$Kpub^{CAP}$: chave pública da CAP $Kpriv^{CAP}$: chave privada da CAP, que ficará armazenada num repositório seguro de informação $Cert_{CAP}{}^{X509}\{SSL\_DATA\}$: Certificado X.509 utilizado para estabelecer ligações seguras (SSL/TLS) entre as diversas entidades do sistema. Este certificado pode ter sido gerado pela própria CAP ou por uma autoridade de

[42] ODRL – *Open Digital Rights Language*

	certificação externa.
ECP	$Kpub^{ECP}$: chave pública da ECP $Kpriv^{ECP}$: chave privada da ECP, que ficará armazenada num repositório seguro de informação
FIP	$Kpub^{FIP}$: chave pública da FIP $Kpriv^{FIP}$: chave privada da FIP, que ficará armazenada num repositório seguro de informação
UCP	$Kpub^{UCP}$: chave pública da UCP $Kpriv^{UCP}$: chave privada da UCP, que ficará armazenada num repositório seguro de informação

4.2.6.2 Certificação da ECP (Transporte)

Ao longo desta fase a ECP obtém uma credencial da CAP que, após a sua instalação, permitirá que a ECP possa estabelecer relações de confiança a nível do canal de comunicação com as restantes entidades do sistema.

Emissor	Receptor	Mensagem	Ligação
ECP	CAP	Envio dos dados pessoais da ECP para a CAP, em conjunto com a sua chave pública, para que seja construído o CSR – *Certificate Signing Request* da ECP. Este procedimento pode ser realizado através de um *browser* de Web, ou então de uma forma *off-line*.	HTTPS / *Off-line*
CAP	ECP	Após a verificação dos dados contidos no CSR da ECP, a CAP emite o certificado SSL/TLS para a ECP ($Cert_{CAP}^{X509}\{SSL\_DATA_{ECP}\}$). Este certificado é depois instalado em todos os componentes que necessitem de estabelecer ligações seguras SSL/TLS (como são o caso de servidores Web e de *peers* OPIMA – cada OVM possui uma credencial com este formato).	HTTPS / *Off-line*

4.2.6.3 Certificação da FIP (Transporte)

Ao longo desta fase a FIP obtém uma credencial da CAP que, após a sua instalação, permitirá que a FIP possa estabelecer relações de confiança a nível do canal de comunicação com as restantes entidades do sistema.

Emissor	Receptor	Mensagem	Ligação
FIP	CAP	Envio dos dados pessoais da FIP para a CAP, em conjunto com a sua chave pública, para que seja construído o CSR – *Certificate Signing Request* da FIP. Este procedimento pode ser realizado através de um *browser* de Web, ou então de uma forma *off-line*.	HTTPS / *Off-line*
CAP	FIP	Após a verificação dos dados contidos no CSR da FIP, a CAP emite o certificado SSL/TLS para a FIP ($Cert_{FIP}^{X509}\{SSL\_DATA_{FIP}\}$). Este certificado é depois instalado em todos os componentes que necessitem de estabelecer ligações seguras SSL/TLS (como são o caso de servidores Web e de *peers* OPIMA – cada OVM possui uma credencial com este formato).	HTTPS / *Off-line*

4.2.6.4 Certificação da UCP (Transporte)

Ao longo desta fase a UCP obtém uma credencial da CAP que, após a sua instalação, permitirá que a UCP possa estabelecer relações de confiança a nível do canal de comunicação com as restantes entidades do sistema. Esta credencial pode ser introduzida pela fabricante da UCP aquando da produção da mesma, pelo que esta fase pode ocorrer antes do utilizador obter e instalar a sua UCP.

Emissor	Receptor	Mensagem	Ligação
UCP	CAP	Envio dos dados pessoais da UCP para a CAP, em conjunto com a sua chave pública, para que seja construído o CSR – *Certificate Signing Request* da UCP. Este procedimento pode ser realizado através de um *browser* de Web, ou então de uma forma *off-line*.	HTTPS / *Off-line*
CAP	UCP	Após a verificação dos dados contidos no CSR da UCP, a CAP emite o certificado SSL/TLS para a UCP ($Cert_{UCP}^{X509}\{SSL\_DATA_{UCP}\}$). Este certificado é depois instalado em todos os componentes que necessitem de estabelecer ligações seguras SSL/TLS (como é o caso do *peer* OPIMA – a OVM do utilizador).	HTTPS / *Off-line*

4.2.6.5 Certificação da ECP (Transaccional)

Após a obtenção da sua primeira credencial da CAP, que permite o estabelecimento de ligações seguras, a ECP irá obter junto da CAP as credenciais necessárias para o estabelecimento de relações de confiança a nível transaccional com as restantes entidades do sistema.

Emissor	Receptor	Mensagem	Ligação
ECP	CAP	A ECP, através de um *browser* de Web, dirige-se a uma CAP e solicita a emissão de uma credencial. A ECP envia a sua chave pública e outros dados pessoais para a CAP: $Kpub_{ECP}$	HTTPS
CAP	ECP	Após uma verificação bem sucedida dos dados fornecidos pela ECP, a CAP emite uma credencial para a ECP: $Cert_{CAP}{}^{XML}\{Kpub_{ECP}\}$	HTTPS

4.2.6.6 Certificação da FIP (Transaccional)

Após a obtenção da sua primeira credencial da CAP, que permite o estabelecimento de ligações seguras, a FIP irá obter junto da CAP as credenciais necessárias para o estabelecimento de relações de confiança a nível transaccional com as restantes entidades do sistema.

Emissor	Receptor	Mensagem	Ligação
FIP	CAP	A FIP, através de um *browser* de Web, dirige-se a uma CAP e solicita a emissão de uma credencial. A FIP envia a sua chave pública e outros dados pessoais para a CAP: $Kpub_{FIP}$	HTTPS
CAP	FIP	Após uma verificação bem sucedida dos dados fornecidos pela FIP, a CAP emite uma credencial para a FIP: $Cert_{CAP}{}^{XML}\{Kpub_{FIP}\}$	HTTPS

4.2.6.7 Certificação da UCP (Transaccional)

Após a obtenção da sua primeira credencial da CAP, que permite o estabelecimento de ligações seguras, a UCP irá obter junto da CAP as credenciais necessárias para o estabelecimento de relações de confiança a nível transaccional com as restantes entidades do sistema.

Emissor	Receptor	Mensagem	Ligação
UCP	CAP	A UCP, através de um *browser* de Web, dirige-se a uma CAP	HTTPS

		e solicita a emissão de uma credencial. A UCP envia a sua chave pública e outros dados pessoais para a CAP: $Kpub_{UCP}$	
CAP	UCP	Após uma verificação bem sucedida dos dados fornecidos pela FIP, a CAP emite uma credencial para a UCP: $Cert_{CAP}{}^{XML}\{Kpub_{UCP}\}$	HTTPS

4.2.6.8 Registo da ECP na FIP (Transaccional)

O objectivo desta transacção é o de permitir que uma ECP possua uma conta válida numa FIP para que esta possa garantir a confiança dos vários UCP numa determinada ECP. Igualmente, permite que a ECP possa estabelecer uma forma válida de processamento dos diversos meios de pagamento fornecidos por um determinado UCP.

Emissor	**Receptor**	**Mensagem**	**Ligação**
ECP	FIP	A ECP, através de um *browser* de Web, dirige-se a uma FIP e solicita o seu registo e consequente emissão de uma credencial. A ECP envia a credencial emitida pela CAP, que contém a sua chave pública, assim como outros dados pessoais (nomeadamente acerca da sua conta bancária) para a FIP: $Cert_{CAP}{}^{XML}\{Kpub_{ECP}\}$+ NIB	HTTPS
FIP	ECP	Após uma verificação bem sucedida dos dados fornecidos pela ECP, nomeadamente da data de validade da credencial, da assinatura digital da CAP e da conta bancária fornecida pelo ECP, a FIP emite uma credencial para a ECP: $Cert_{FIP}{}^{XML}\{Kpub_{ECP}\}$	HTTPS

4.2.6.9 Registo da UCP na FIP (Transaccional)

O objectivo desta transacção é o de permitir que uma UCP possua um meio de pagamento válido numa FIP para que esta possa garantir a confiança das várias ECP numa determinada UCP. Igualmente, permite que a UCP possa estabelecer um meio válido de pagamento dos diversos conteúdos digitais que a ECP lhe fornece.

Emissor	**Receptor**	**Mensagem**	**Ligação**
UCP	FIP	A UCP, através de um *browser* de Web, dirige-se a uma FIP e solicita o seu registo e consequente emissão de uma	HTTPS

		credencial. A UCP envia a credencial emitida pela CAP, que contém a sua chave pública, assim como outros dados pessoais (nomeadamente acerca do meio de pagamento a fornecer, por exemplo, o seu cartão de crédito) para a FIP: $Cert_{CAP}{}^{XML}\{Kpub_{ECP}\}$+ MP	
FIP	UCP	Após uma verificação bem sucedida dos dados fornecidos pela UCP, nomeadamente da data de validade da credencial, da assinatura digital da CAP e do meio de pagamento da UCP, a FIP emite uma credencial para a UCP: $Cert_{FIP}{}^{XML}\{Kpub_{UCP}\}$	HTTPS

4.2.6.10 Inscrição da UCP na ECP (Transaccional)

Para que o utilizador possa efectuar aquisições de conteúdo na ECP, necessita de estar registado nesta. Normalmente o processo de registo numa ECP tradicional baseia-se no estabelecimento de um registo que depende do conjunto nome de utilizador e palavra-chave para autenticar o utilizador. De igual forma, a confiança é estabelecida individualmente entre o utilizador e a ECP, não existindo nenhuma garantia à partida por parte da ECP de que os utilizadores são válidos e "honestos" nem de que o meio de pagamento fornecido pelo mesmo é de confiança e é válido. No caso do sistema apresentado, existe uma terceira entidade, a FIP, que garante à ECP que os dados fornecidos pelo utilizador são válidos e que, consequentemente, o meio de pagamento apresentado também o será. Adicionalmente, ao utilizador são apresentadas provas de confiança por parte da ECP que permitem que o utilizador possa confiar na ECP. Os verdadeiros dados de pagamento nunca são na verdade apresentados à ECP, assim como a verdadeira identidade do utilizador também não é revelada.

Para inscrição na ECP, o utilizador entrega as credenciais fornecidas pela FIP, as quais a ECP verifica, registando-o e solicitando-lhe a introdução de uma palavra-chave que lhe permite a aquisição de conteúdo digital.

Emissor	**Receptor**	**Mensagem**	**Ligação**
UCP	ECP	O utilizador acede a uma página de registo da ECP através de um *browser* de Web. O utilizador fornece ao ECP a credencial que foi obtida a partir de uma FIP: $Cert_{FIP}{}^{XML}\{Kpub_{UCP}\}$. Após a verificação das credenciais apresentadas pela UCP, a ECP regista o utilizador (cuja identificação virtual (nome de utilizador) está incrustado no certificado) solicitando-lhe a introdução de uma palavra-chave. O utilizador fornece esta	HTTPS

		palavra-chave.	
ECP	UCP	Após a introdução de todos estes dados por parte do utilizador e da sua consequente verificação e registo por parte da ECP, esta envia uma mensagem à UCP (apresentada na janela do *browser* de Web), indicando que o utilizador se encontra registado na ECP e que pode passar a adquirir conteúdo digital na mesma.	HTTPS

4.2.6.11 Aquisição de conteúdo na ECP por parte da UCP (Transaccional)

Sempre que um utilizador registado deseja adquirir um determinado conteúdo numa ECP deve escolher qual o conteúdo que deseja e depois negociar os termos de utilização do mesmo (para o caso de conteúdos digitais), o que leva à correspondente produção de uma licença para o conteúdo em causa. Para que a negociação possa ser bem sucedida é necessário que o utilizador prove que está efectivamente registado na ECP, utilizando para isso o nome do utilizador e correspondente palavra-chave configuradas no passo anterior.

Emissor	**Receptor**	**Mensagem**	**Ligação**
UCP	ECP	O utilizador, fazendo uso do seu *browser* de Web, navega pelo *site* da ECP para escolher os seus conteúdos digitais. O utilizador selecciona um determinado conteúdo (neste caso particular um conteúdo multimédia em formato MP4).	HTTP
UCP	ECP	Aquando da escolha do conteúdo no *site* ECP, o utilizador inicia um processo de negociação para a utilização do conteúdo digital em causa. O utilizador pode escolher algumas de entre as condições de utilização existentes (nomeadamente o número de vezes que o conteúdo pode ser tocado e quantas vezes poderá ser copiado). Após a escolha do utilizador este fornecerá o seu nome de utilizador e correspondente palavra-chave, e o ECP produzirá uma correspondente licença para o conteúdo que ficará armazenada na ECP para posterior acesso via sistema IPMP.	HTTPS
UCP	ECP	O utilizador descarrega o ficheiro MP4 que se encontra protegido. A ligação entre a ECP e UCP nesta fase não necessita de estar protegida, uma vez que o próprio conteúdo já se encontra encriptado e protegido.	HTTP

4.2.6.12 Descarregamento do sistema IPMP (Transaccional)

Quando o utilizador tenta abrir um conteúdo MP4 protegido, a UCP analisa o conteúdo e verifica que este está protegido. Ao consultar as regras que se encontram embebidas no conteúdo (regras de conteúdo), o sistema verifica quais são os sistemas IPMP que são aplicáveis a este. Caso o sistema IPMP não esteja disponível na UCP, este é descarregado da ECP, através de um SAC.

Emissor	Receptor	Mensagem	Ligação
ECP	UCP	Descarregamento seguro do sistema de IPMP realizado através do OPIMA SAC. Após o sistema de IPMP ter sido descarregado é inicializado pela UCP.	OPIMA SAC

4.2.6.13 Descarregamento da Licença do conteúdo (Transaccional)

Após ter sido inicializado, o sistema de IPMP verifica o ficheiro com o conteúdo MP4 protegido, solicitando à OVM a verificação da existência de uma licença apropriada para efectuar a visualização do conteúdo. Caso esta licença se encontre já disponível na UCP, esta é utilizada. No caso dessa licença ainda não estar presente na UCP, torna-se necessário o seu descarregamento a partir da ECP.

Emissor	Receptor	Mensagem	Ligação
UCP	ECP	A UCP através do sistema de IPMP e OVM requisita uma licença para a visualização de um determinado conteúdo previamente descarregado ($REQ^{XML}\{C_{id}+UCP_{id}\}$)	OPIMA SAC
ECP	UCP	A ECP verifica o pedido realizado pela UCP (nomeadamente, a assinatura digital da ECP, a identificação do conteúdo e a identificação da UCP) e emite a correspondente licença para o conteúdo especificado ($Cert_{ECP}{}^{XML}\{LIC[C_{id}+UCP_{id}+UR_{play}+UR_{copies}+C_{key}+Value]\}$).	OPIMA SAC

4.2.6.14 Envio de autorização de pagamento (Transaccional)

Apenas após a recepção da licença por parte da UCP, é produzida uma credencial com uma autorização de pagamento da UCP que é enviada depois para a ECP. Nenhuma destas transacções revela qualquer informação acerca da identidade real do utilizador e dos seus meios de pagamento. Estas transacções financeiras vão sendo registadas pela ECP e são depois enviadas para a correspondente FIP que as processará (transferências de fundos entre os utilizadores e as ECP).

Emissor	Receptor	Mensagem	Ligação
UCP	ECP	A UCP prepara e envia para a ECP a correspondente autorização para o pagamento do valor solicitado pelo serviço	SSL/TLS

		prestado pela ECP ($Cert_{UCP}^{XML}${PAYdata[U_{id}+Value]})	

4.2.6.15 Envio das autorizações de pagamento para a FIP (Transaccional)

As diversas autorizações de pagamento registadas pelas ECP são armazenadas e mais tarde são enviadas em lote para a correspondente FIP, que se encarregará de as verificar e de processar as correspondentes transacções financeiras.

Emissor	Receptor	Mensagem	Ligação
ECP	FIP	Temporariamente a ECP envia as autorizações de pagamento obtidas das UCP para a FIP ($Cert_{ECP}^{XML}${$Cert_{UCP}^{XML}${PAYdata[U_{id}+Value]}}). A FIP verifica os dados enviados pela ECP e processa as consequentes transacções financeiras.	SSL/TLS

Em anexo (Anexo C) pode ser encontrado um Diagrama de Sequência em UML que especifica todas as fases do protocolo descritas acima. Pode igualmente ser consultado em anexo (Anexo D) a definição em formato XML DTD e *Schema* de todas as mensagens e credenciais do sistema OpenSDRM.

4.3 Arquitectura PKI do sistema OpenSDRM

Ao longo desta secção são apresentadas esquematicamente ambas as arquitecturas PKI (de confiança) que são utilizadas pelo sistema OpenSDRM.

São apresentadas duas arquitecturas: (a) uma primeira, relacionada com a protecção das comunicações entre as entidades que são responsáveis pela emissão de credenciais que permitem o estabelecimento de canais de comunicação seguros e autenticados (SSL/TLS) (ver secção 2.6.2 e secção 4.2), e (b) outra relacionada com a segurança transaccional que emite credenciais XML para as entidades que efectuam transacções entre si (ver secção 4.2).

Uma vez que grande parte dos componentes do sistema OpenSDRM se baseia em comunicações seguras SSL/TLS, estes necessitavam de possuir um certificado X.509 que lhes permitiria estabelecer a autenticação e comunicação segura entre si (isto ao nível de comunicações). Para que todas estas entidades possam obter estes certificados, precisam de recorrer aos serviços de uma CAP (ou várias). Como teremos oportunidade de verificar (ver secção 4.3.1) estes certificados podem ser emitidos directamente para entidades finais (no caso das ECP e das FIP) ou para outras Autoridades de Certificação (no caso dos produtores de OVM (FOVM) ou de sistemas IPMP (FIPMP)).

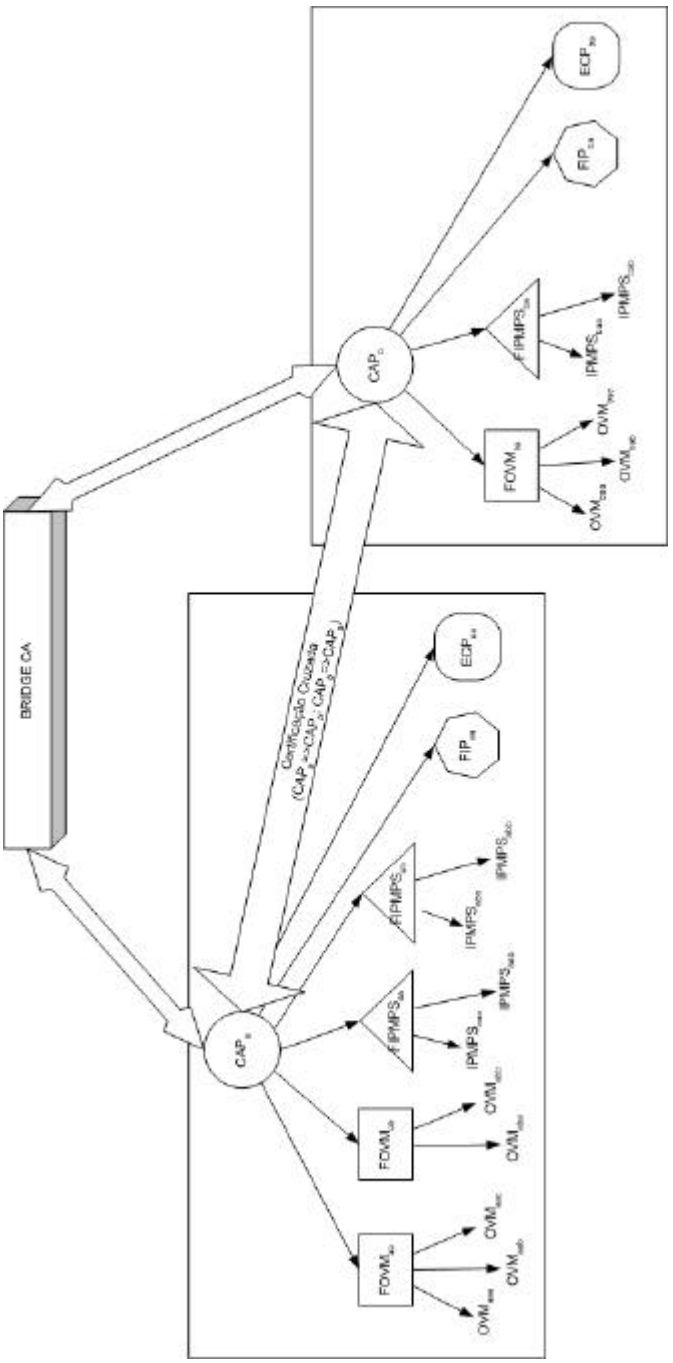
De igual forma, as transacções realizadas entre alguns dos componentes eram baseadas em mensagens formatadas em XML (ECP, *Wallets* e FIP). Estas mensagens eram assinadas digitalmente pelas entidades que as criavam e usavam o protocolo SSL/TLS para serem transferidas com segurança entre si. Para a criação e verificação destas assinaturas digitais, as entidades necessitavam de possuir certificados digitais

XML. A emissão destes certificados digitais estava atribuída a uma CAP (ou várias). Estes certificados digitais eram emitidos para ECPs, *Wallets* e FIPs.

Apesar de serem apresentadas arquitecturas distintas, estas podem ser facilmente fundidas numa única arquitectura no caso da CAP ser híbrida e de ter a capacidade de emitir em simultâneo credenciais em formato X.509 e XML.

4.3.1 Arquitectura PKI baseada em X.509

A arquitectura PKI X.509 adoptada pode utilizar tanto o modelo de Arquitectura Distribuída de Confiança ou Modelo em Rede (ver Capítulo 2). Esta organiza as entidades emissoras de credenciais numa estrutura hierárquica que emite certificados para as entidades que precisam destes para estabelecer comunicações seguras entre si: Fabricantes de OVMs, Fabricantes de IPMPs, FIPs e ainda ECPs (Figura 4.12). A entidade responsável pela emissão destas credenciais é a CAP, sendo que as relações entre as diversas entidades certificadas dependem da confiança estabelecida entre cada uma delas e a CAP (por exemplo, OVM_{aaa}:CAP_a=>$FOVM_{aa}$=>OVM_{aaa} pode estabelecer uma relação de confiança com o $IPMPS_{aab}$:CAP_a=>$FIPMPS_{aa}$=>$IPMPS_{aab}$).



BRIDGE CA CA ponte que serve para efectuar a ligação entre CAs distintas;
CAP Plataforma de Autoridade de Certificação
FOVM Fabricante de OVMs
FIPMPS Fabricantes de IPMPs
FIP Plataforma da Instituição Financeira
ECP Plataforma de Comércio Electrónico
OVM Máquina Virtual OPIMA
IPMPS Sistema IPMP

Figura 4.12 Arquitectura de PKI da Segurança das Comunicações

No entanto, é possível que exista a necessidade de que entidades que possuam credenciais obtidas a partir de CAPs distintas desejem estabelecer relações de confiança entre si. Neste caso, e uma vez que ambas as entidades dependem da confiança que detém na sua própria CAP, então não é possível estabelecer um relacionamento de confiança (é o caso por exemplo, em que a OVM_{aac}:CAP_a=>$FOVM_{aa}$=>OVM_{aac} não pode estabelecer a relação de confiança com o $IPMPS_{bab}$:CAP_b=>$FIPMPS_{ba}$=>$IPMPS_{bab}$).

A solução para este problema reside na opção de uma de duas soluções técnicas possíveis: (1) que ambas as CAPs realizem uma certificação cruzada entre si ([CAP_a=>CAP_b] e [CAP_b=>CAP_a]) ou então (2) que exista uma CA ponte que sirva de ponto comum de certificação entre ambas as CAPs ([CA-BRIDGE=>CAP_a] e [CA-BRIDGE=>CAP_b]).

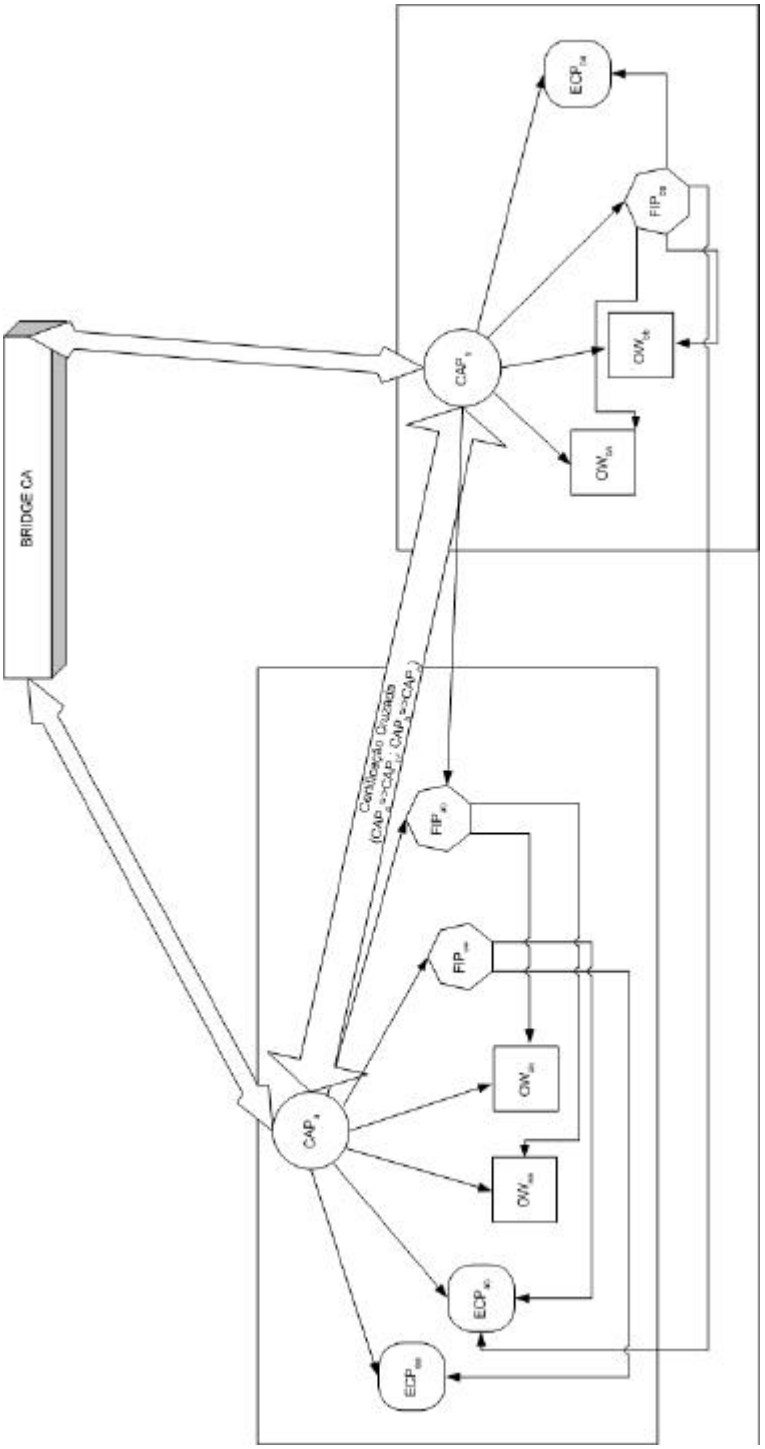
Através da utilização de uma das metodologias citadas é possível o estabelecimento da confiança entre entidades que possuam certificados de CAPs distintas. No exemplo acima citado já é então possível estabelecer confiança entre a OVM_{aac} e o $IPMPS_{bab}$, através de uma das seguintes formas:

- Com certificação cruzada:
    - OVM_{aac}:[CAP_a=>CAP_b ;CAP_b=>CAP_a]=>CAP_a=>$FOVM_{aa}$=>OVM_{aac}
    - $IPMPS_{bab}$: [CAP_a=>CAP_b ;CAP_b=>CAP_a]=>$FIPMPS_{ba}$=>$IPMPS_{bab}$
- Com uma CA ponte:
    - OVM_{aac}: [CA-BRIDGE=>CAP_a;CA-BRIDGE=>CAP_b]=>$FOVM_{aa}$=>OVM_{aac}
    - $IPMPS_{bab}$:[CA-BRIDGE=>CAP_a;CA-BRIDGE=>CAP_b]=>$FIPMPS_{ba}$=>$IPMPS_{bab}$

4.3.2 Arquitectura PKI baseada em XML

A arquitectura PKI XML utiliza o modelo de Arquitectura Distribuída de Confiança (ver Capítulo 2). Esta organiza as entidades emissoras de credenciais numa estrutura hierárquica (com algumas excepções) que emitem certificados para as entidades que precisam destes para estabelecer confiança nas transacções que realizam entre si: *Wallets*, ECPs e FIPs (Figura 4.13).

A entidade responsável pela emissão destas credenciais é a CAP, sendo que as relações entre as diversas entidades certificadas dependem da confiança estabelecida entre cada uma delas e a CAP (por exemplo, OW_{aa}:CAP_a=>OW_{aaa} pode estabelecer uma relação de confiança com a FIP_{ab}:CAP_a=>FIP_{ab}).



BRIDGE CA CA ponte que serve para efectuar a ligação entre CAs distintas
CAP Plataforma de Autoridade de Certificação
OW *Wallets* das UCPs
FIP Plataforma da Instituição Financeira
ECP Plataforma de Comércio Electrónico

Figura 4.13 Arquitectura PKI da segurança Transaccional

A FIP é igualmente responsável por emitir credenciais para *Wallets* e para ECPs. Estas credenciais permitem que possa ser estabelecida confiança entre as *Wallets* e os ECPs nas transacções financeiras realizadas entre ambos.

Apesar de em termos de implementação do sistema OpenSDRM apenas ter sido utilizada uma única CAP e uma única FIP podem existir situações em que mais que uma CAP ou FIP possam existir e em que ECPs e

Wallets certificadas por CAPs e/ou FIPs diferentes possam realizar transacções entre si. Para solucionar este tipo de problemas podem ser adoptadas três abordagens distintas, quer a nível das CAPs, quer ao nível das FIPs:

- A nível das CAPs:
    - Ambas as CAPs realizam entre si uma certificação cruzada: [CAP_a=>CAP_b; CAP_b=>CAP_a];
    - Ambas as CAPs recorrem à utilização de uma CA ponte: [BRIDGE-CA=>CAP_a; BRIDGE-CA=>CAP_b];
    - Ambas as CAPs podem certificar a mesma entidade: [CAP_a=>Entidade, CAP_b=>Entidade]
- A nível das FIPs:
    - Ambas as FIPs dependem da mesma CAP:
        - CAP_a=>FIP_{aa}=>OW_{aa}
        - CAP_a=>FIP_{aa}=>ECP_{ab}
    - As FIPs dependem de CAPs diferentes, mas com certificação cruzada entre si:
        - [CAP_a=>CAP_b;CAP_b=>CAP_a]=>FIB_{aa}=>OW_{aa}
        - [CAP_a=>CAP_b;CAP_b=>CAP_a]=>FIB_{aa}=>ECP_{ab}
    - As FIPs dependem de CAPs diferentes, com uma CA ponte:
        - [CA-BRIDGE=>CAP_a;CA-BRIDGE=>CAP_b]=>FIB_{aa}=>OW_{aa}
        - [CA-BRIDGE=>CAP_a;CA-BRIDGE=>CAP_b] =>FIB_{aa}=>ECP_{ab}
    - As FIPs dependem de CAPs diferentes, mas uma delas tem no caminho de certificação uma CAP em comum:
        - CAP_a=>FIP_{aa}=>OW_{aa}
        - [CAP_a=>FIP_{aa};CAP_b=>FIP_{aa}]=>ECP_{ab}

Este capítulo apresentou a criação e adaptação de uma plataforma distribuída de segurança, designada por PKI, ao sistema OCCAMM. O novo sistema, OpenSDRM, conferiu ao OCCAMM as necessárias funcionalidades de segurança que haviam sido identificadas, assim como permitiu a integração das funcionalidades DRM existentes e a criação de novas. Foi igualmente descrito um sistema IPMP alternativo baseado em *Wallets* que funciona de forma integrada com esta plataforma, servindo igualmente como sistema de pagamento. Foi de igual forma desenhada a arquitectura das PKI usadas. Todo este sistema foi

implementado e é apresentado no Anexo H.

A concepção deste sistema visou colmatar algumas das lacunas identificadas, quer na iniciativa OPIMA, quer no OCCAMM em termos de segurança. Entenda-se por segurança, neste contexto, um conjunto de funcionalidades que proporcionam confidencialidade, integridade, autenticação e não repúdio às entidades do sistema. Identificadas como um requisito dos sistemas DRM modernos [STDM01], as PKI, são indispensáveis, devendo existir uma convergência tecnológica entre ambas. Apenas assim podem ser oferecidas as garantias necessárias para a protecção efectiva de:

- Autores de Conteúdo (recebimento dos respectivos valores dos direitos de autor);
- Conteúdos (protecção e integridade dos conteúdos e das suas regras de utilização);
- Fornecedores de Conteúdo (recebimento pelos conteúdos que comercializam);
- Utilizadores (integridade dos conteúdos, pagamentos seguros, integridade e segurança das regras de utilização dos mesmos).

O sistema OpenSDRM implementado oferece estas garantias, proporcionando a integração entre o sistema DRM e PKI.

O sistema apresentado esteve em funcionamento em paralelo com os testes do projecto OCCAMM, sendo que os dois sistemas IPMP eram perfeitamente interoperáveis entre si (um conteúdo protegido poderia ser controlado quer pela versão proprietária do sistema IPMP, quer pela versão não-proprietária desenvolvida aqui). No entanto, e apesar de serem interoperáveis ao nível do conteúdo, o sistema IPMP proprietário usava o sistema tradicional OCCAMM sem fazer recurso a uma PKI, enquanto que o sistema IPMP não proprietário baseado em Wallet, usava o sistema OpenSDRM. A tabela seguinte resume as principais diferenças entre os dois:

Sistema IPMP (*CryptoWorks*)	**Sistema IPMP (*Wallet*)**
Baseado em cartões inteligentes, para armazenar informação em segurança	Baseado em software alojado no sistema do cliente (*Wallet*) para armazenar informação em segurança
Necessário a instalação de *hardware* (leitor de cartões inteligentes) e *software* (controladores) adicionais.	Necessário apenas a instalação de *software* (*Wallet*).
Obtinha as licenças encriptadas, mas não autenticava os intervenientes nas transacções	Realizava a autenticação dos intervenientes nas transacções e obtinha as licenças encriptadas
Não servia como sistema de pagamento	Era usada como sistema de pagamento genérico
O dispositivo cartão inteligente é bastante seguro e de ataque difícil	Pode ser sujeito a ataques de força bruta
Não era baseado em PKI	Totalmente dependente de uma PKI

Tabela 4.1 Diferenças entre os dois sistemas IPMP

No próximo capítulo, será apresentado um dos testes realizados ao sistema, integrado nos testes de comercialização de música digital *on-line*.

5 EXEMPLO DE UTILIZAÇÃO E RESULTADOS

5.1 Introdução

O objectivo do presente capítulo consiste na apresentação de uma descrição detalhada e passo-a-passo das interacções entre os diversos componentes e as ferramentas que constituem a arquitectura definida para os testes de utilização real. A plataforma de testes é composta por todo o sistema que foi desenvolvido no âmbito do projecto OCCAMM [OCBMS00, OCIOSF01], assim como o sistema IPMP baseado em *Wallet* e a correspondente arquitectura PKI/DRM desenvolvidos no âmbito desta dissertação e que constituem o sistema OpenSDRM. Todas estas interacções serão seguras, quer através de protocolos específicos (OPIMA SAC), quer através da norma SSL/TLS em concordância com o que foi descrito nos capítulos anteriores (Capítulo 3 e Capítulo 4).

Conforme o que se havia referido no capítulo anterior, um dos testes de utilização, que foi levado a cabo pelo projecto OCCAMM, para validar os resultados da implementação OVM pelo projecto OCCAMM, do sistema IPMP (baseado em *Wallet*) e da PKI e DRM desenvolvidos, teve por objectivo a comercialização de música em formato digital.

Este teste era particularmente importante na medida em que o mercado de comercialização de música sofre uma revolução [TCFMI00, DMPP01] (no Anexo G pode ser encontrada uma descrição sobre o sector da música). Esta revolução é provocada por todos os problemas inerentes da pirataria que se verifica hoje em dia na Internet, que oferece a possibilidade de milhões de utilizadores poderem obter música em formato digital (MP3) com qualidade quase idêntica à do CD com bastante facilidade [TCFMI00, MP3BMD00].

De igual forma, o grande desenvolvimento das tecnologias P2P permitiu que os utilizadores pudessem partilhar a partir do seu próprio computador pessoal todo tipo de ficheiros e, em especial, ficheiros contendo faixas de música. Igualmente, a crescente proliferação dos leitores e gravadores de CDs nos computadores pessoais, assim como a facilidade de obtenção de software que permita criar cópias em formato digital das faixas de música dos CDs originais (vulgarmente designado por software de "*ripping*") vieram contribuir para o aumento da pirataria [DMPP01]. Após terem sido copiadas e comprimidas em formatos como o MP3, as faixas de música são facilmente distribuídas através da Internet, sem quaisquer tipo de preocupações para com os direitos de autor.

Outra das tendências que se observa actualmente é o aparecimento de dispositivos domésticos que permitem aos utilizadores escutar música sem que para isso necessitem de um computador pessoal (leitores portáteis de MP3, PDAs, telemóveis, leitores de DVD e MP3) o que levou a uma maior disseminação e proliferação do MP3 [TCFMI00, DMPP01]. Um dos primeiros dispositivos deste género foi introduzido pela *Diamond Multimedia*, designado por *Rio Player*, o que causou reacções imediatas por parte da RIAA –

Recording Industry Association of América, nomeadamente, o levantamento de um processo judicial à *Diamond*, tentando impedi-la de realizar o lançamento [DMPP01].

Este modelo de distribuição de música em formato digital é hoje em dia o mais utilizado na Internet [TKPWOLMD01], algo que provoca, quer nos autores, quer nas editoras discográficas grande preocupação, pelas elevadas perdas financeiras que lhes têm sido infligidas (cerca de um quarto dos americanos já descarregaram música em formato digital e/ou escutaram rádio através da Internet). Estes actores debatem-se nos nossos dias com um dilema muito significativo: se por um lado encaram como promissora e oportuna a utilização da Internet como uma nova forma de promoção de música e como canal de distribuição e comercialização da mesma, por outro consideram-na como uma séria ameaça ao seu modelo de negócios tradicional [MP3BMD00, TKPWOLMD01].

Os testes de utilização real que vão ser descritos neste capítulo utilizaram a seguinte infra-estrutura técnica:

- Plataforma cliente (UCP) baseada no OPIMA, desenvolvida pelo projecto OCCAMM, que inclui:
    - OVM, desenvolvida pelo projecto OCCAMM (Capítulo 3);
    - Aplicação para visualizar o conteúdo em formato MPEG-4, desenvolvida pelo projecto OCCAMM (Capítulo 3);
    - Sistema IPMP baseado em *Wallet*, desenvolvido no âmbito desta dissertação (Capítulo 4);
    - *Wallet* desenvolvida no âmbito desta dissertação (Capítulo 4).
- Plataforma de produção de conteúdo protegido, desenvolvida no âmbito do projecto OCCAMM (Capítulo 3);
    - Produtor de conteúdo MPEG-4 protegido;
    - Servidor de conteúdos multimédia;
- Plataforma mista PKI/DRM (OpenSDRM) desenvolvida no âmbito desta dissertação (Capítulo 4), que inclui:
    - Plataforma de Certificação (CAP) (ferramentas de emissão e gestão de certificados digitais X.509 e XML);
    - Plataforma de Comércio Electrónico (ECP), que inclui:
        - *Site* de Web da Loja electrónica, desenvolvida no âmbito do OCCAMM, mas adaptada nesta dissertação para usar o OpenSDRM;
        - Servidor de Licenças, desenvolvida nesta dissertação;
        - Servidor de Sistemas IPMP, desenvolvida no âmbito do OCCAMM, mas adaptada nesta dissertação para usar o OpenSDRM.
    - Plataforma Financeira (FIP), que inclui:
        - Ferramenta para processar pagamentos OpenSDRM (TTP), desenvolvida no âmbito desta dissertação;

- Processador de Pagamentos (*Payment Gateway*) utilizado para fazer a interface com o sistema de pagamentos real, que não foi desenvolvido.

Todos estes elementos citados permitiram a realização dos testes de utilização real dos mesmos, através da simulação de um serviço de consumo de música em formato digital, utilizando um modelo de negócios específico.

A realização destes testes pretendia obter a verificação:

- da adesão dos diversos actores do sector musical a esta iniciativa de distribuição e consumo de música digital através da Internet (nomeadamente autores, editoras e consumidores finais);
- da facilidade de utilização de toda a infra-estrutura desenvolvida por parte dos actores citados no ponto anterior;
- da segurança do sistema e a sua mais valia na protecção efectiva do conteúdo disponibilizado;
- e prova que o sistema garante o pagamento e o consumo condicional do conteúdo em causa.

É apresentada uma descrição dos testes realizados assim como a integração dos mesmos num dos modelos de distribuição possíveis para a música digital. De seguida, será apresentado o método de avaliação do teste assim como as principais conclusões e resultados extraídos da realização do mesmo.

5.2 Testes de Aquisição e Consumo Seguro de Música Digital

Os testes de utilização real de aquisição e consumo seguro de música em formato digital foram baseados em dois modelos de distribuição de música digital: o modelo de descarregamento e o modelo de fluxo contínuo (ver Anexo G para uma análise dos diversos modelos de distribuição de música digital). Estes modelos são os que detêm uma maior representatividade no mercado da distribuição de música digital dos nossos dias [OCOLSMD00].

Casos como os formatos *Real Áudio* (.ra), da *Real Networks*, o *Windows Media Format* (.wma), do *Windows Media Player*, do MP3(.mp3) ou ainda do recente *Ogg-Vorbis* (.ogg), têm uma das suas principais aplicações na rádio em tempo real através da Internet [OCOLSMD00, OCOOSS01], em que o modelo de distribuição que está presente é o modelo de fluxo contínuo ou de *streaming*. Um exemplo típico deste modelo é o caso do *site* do portal IOL, COTONETE (http://www.cotonete.iol.pt), que permite que os utilizadores possam criar as suas próprias emissões de rádio através da Internet (Figura 5.2).

Figura 5.1 O *site* de Web do Cotonete

Apesar de tudo, o modelo de distribuição mais comum hoje em dia continua a ser o modelo de Descarregamento, que pode ser encontrado em grande parte dos *sites* de Web e em grande parte das aplicações P2P. Como exemplos desta forma de distribuição o MP3.com e o *AudioGalaxy*, entre outros (Figura 5.3).

Figura 5.2 *Site* do MP3.com e a aplicação P2P *AudioGalaxy*

5.2.1 Conteúdo

O conteúdo para os testes foi composto por uma série de ficheiros de música digital de vários estilos, géneros e países. Grande parte da música utilizada nos testes foi fornecida por uma editora discográfica do Reino Unido: a V2 (http://www.v2music.com) (Figura 5.4).

Figura 5.3 O *site* de Web da V2

O conteúdo foi preparado especificamente para os testes da seguinte forma: foi introduzida uma marca de água nas faixas de aúdio, a música foi convertida para o formato AAC – *Advanced Audio Encoding*, foi introduzida meta-informação (informação acerca do sistema IPMP a ser utilizado na protecção) e finalmente foi gerado o *bit stream* em formato MPEG-4. Estas faixas foram depois transferidas e armazenadas num Servidor de Conteúdo que foi utilizado para responder a pedidos enviados pela ECP [OCIOSF01, OCIMPATP01].

Comparativamente ao MP3, o formato AAC oferece uma melhor qualidade de reprodução do áudio, necessitando de cerca de menos 50% de dados, conseguindo obter um rácio de compressão mais elevado. Em termos gerais, a música em formato AAC soa melhor, é descarregada mais rapidamente e ocupa menos espaço de armazenamento ou largura de banda [KBMP3AAC]. O AAC tem vindo a assumir-se como o sucessor "natural" do formato MP3.

5.2.2 Licenciamento

Todo o conteúdo (faixas de áudio) estava sujeito a licenças que descreviam diversos modelos de negócios associados a diferentes condições de utilizações do conteúdo:

- Limite de tempo: permite que um utilizador possa tocar uma faixa musical durante um período de tempo específico. Nos testes realizados as seguintes condições de limite de tempo encontravam-se disponíveis:
    - 1 semana
    - 1 mês
- Limite do número de utilizações: permite que um utilizador possa especificar o número de vezes que o conteúdo pode ser reproduzido. As seguintes condições deste tipo foram especificadas para os testes de música:
    - 3 vezes
    - 20 vezes
- Utilização indefinida: permitem que um utilizador possa adquirir uma licença que permitiria que um determinado conteúdo pudesse ser escutado indefinidamente.

O teste de música utilizava o sistema IPMP que foi descrito no capítulo anterior (Capítulo 4), para controlar o acesso ao conteúdo, segundo a licença que foi adquirida e descarregada pelo utilizador, e para efectuar o pagamento dessa mesma licença. O processo de criação das licenças foi igualmente especificado no anterior capítulo. Estas licenças foram definidas em formato XML (o esquema DTD e o correspondente *XML Schema* é apresentado no Anexo D). Estas são apenas algumas das condições estabelecidas para o teste específico realizado, podendo mais condições ser acrescentadas no formato da licença. O formato de licença adoptado baseia-se em XML e implementa um subconjunto da norma ODRL 1.0 (*Open Digital Rights Language*) [ODRLSP01].

5.2.3 A execução dos testes

Ao longo desta secção são apresentadas as diferentes fases que correspondem à execução dos testes de comercialização *on-line* de música em formato digital protegida. Ao longo da mesma são apresentadas algumas imagens (capturas de ecrã) que ajudam a exemplificar cada uma das fases.

Na figura seguinte (Figura 5.5) encontra-se a descrição gráfica das diferentes fases de execução dos testes de utilização real.

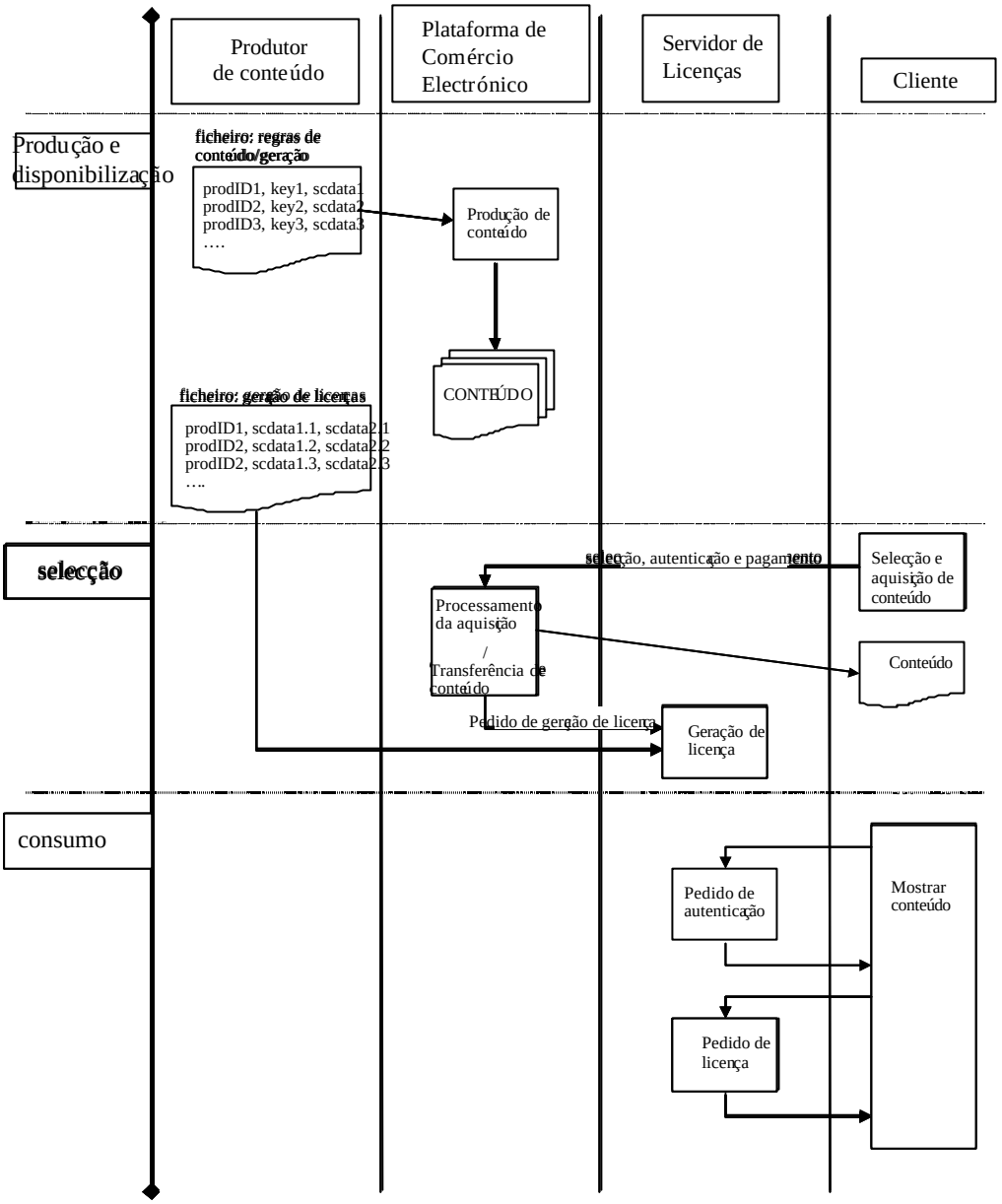


Figura 5.4 Execução dos teste de Música

5.2.3.1 Produção de Conteúdo

O conteúdo utilizado nos testes utiliza o formato MPEG-4. Este formato baseia-se no conceito de componentes orientados por objectos. Cada objecto dentro de um ficheiro MPEG-4 é conhecido por átomo. A descrição das propriedades individuais de cada um destes átomos está fora do âmbito desta dissertação, no entanto, podem ser encontrados mais detalhes sobre as mesmas no documento "ISO/IEC JTC 1/SC 29/WG 11 N4668 subpart 4" [OMPEG4S02].

Cada parte do conteúdo designa-se por *Elementary Streams*, estando associado a um *Elementary Stream Descriptor* (*ES Descriptor*). Os *ES Descriptors* estão agrupados por sua vez em unidades lógicas designadas por *Object Descriptors*, que descrevem um conjunto semelhante de itens de conteúdo.

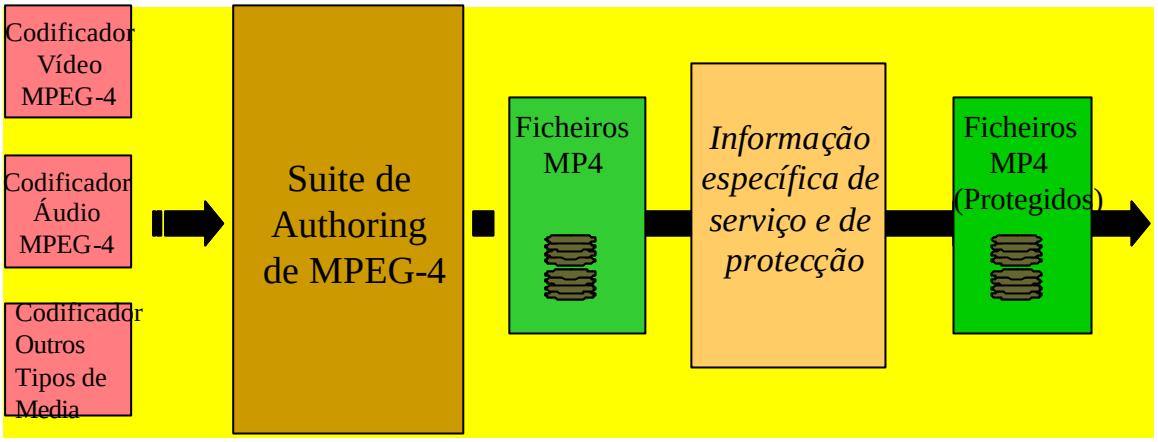


Figura 5.5 Processo de Produção do conteúdo digital para os testes

Para produzir o conteúdo utilizado nos testes foram empregues ferramentas de *authoring* de MPEG-4, que permitiram a criação de *templates* que foram utilizados depois para automatizar o processo de produção do conteúdo. Estes *templates* eram compostos por dois *Elementary Streams*: um contendo áudio enquanto que o outro continha uma imagem JPEG com a foto do álbum e/ou do artista [OCIMPATP01].

Após a produção do ficheiro em formato MP4, este era preparado para conter informação acerca da ferramenta IPMP (nome da ferramenta, URI[43] onde poderá ser obtida, identificador único da mesma) utilizada para o proteger. No fim, o ficheiro era ainda encriptado por uma chave secreta (AES) (Figura 5.6).

Figura 5.6 Ferramenta utilizada na produção do conteúdo

A ferramenta de produção do conteúdo (Figura 5.7) recebe um ficheiro de música em formato WAV/AAC/MP3 em conjunto com um ficheiro JPEG. Estes, em conjunto com uma chave AES, produziam como resultado um ficheiro MPEG-4 protegido. Era igualmente criado um ficheiro adicional: um ficheiro XML que continha a informação necessária para catalogar o conteúdo na ECP (Figura 5.8) [OCIMPATP01].

[43] *Uniform Resource Identifier*

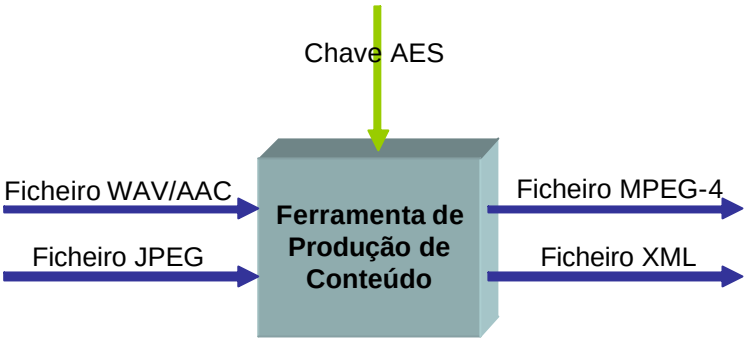


Figura 5.7 Produção dos ficheiros MP4

Concluído este processo, o conteúdo estava preparado para ser colocado na ECP.

5.2.3.2 Disponibilização de Conteúdo

Após a fase de produção de conteúdo este era disponibilizado através da ECP e de um servidor Multimédia. Este último era utilizado para entregar o conteúdo ao cliente. Esta entrega poderia ocorrer de várias formas: através de difusão, através da Web (HTTP) ou de uma forma interactiva (Figura 5.9).

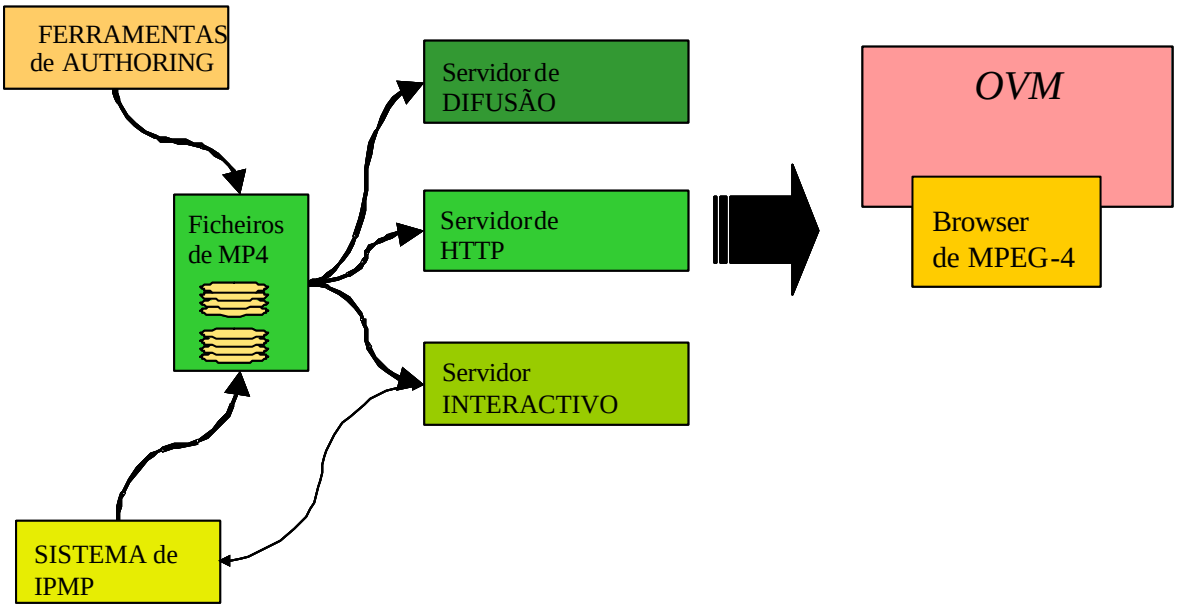


Figura 5.8 Sequência de disponibilização de conteúdo

O cliente precisará de um *Player* de MPEG-4 e de uma OVM para poder descodificar correctamente o conteúdo e desfrutar do mesmo.

5.2.3.3 Certificação do Utilizador numa Autoridade de Certificação

Para que o utilizador pudesse desfrutar do conteúdo recorrendo ao sistema OpenSDRM aqui descrito, deveria ter instalado no seu computador uma aplicação cliente a funcionar sobre uma OVM, assim como, uma *Wallet* que lhe permitirá armazenar os seus dados em segurança (Capítulo 4).

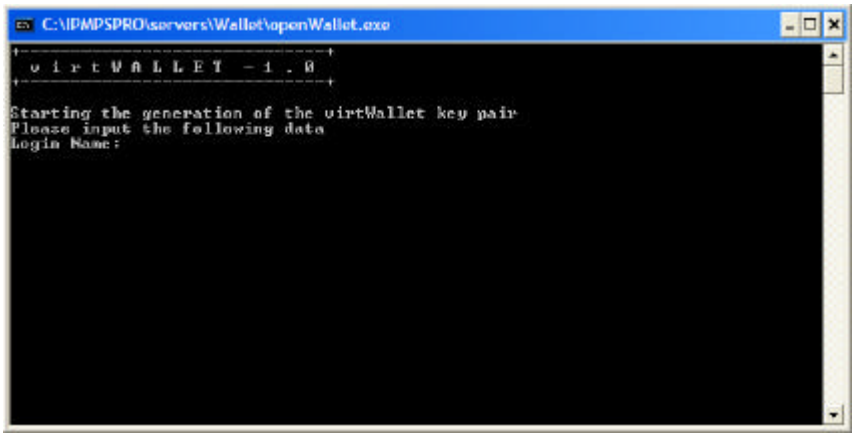


Figura 5.9 Inicialização da *Wallet* por parte do utilizador

Ao iniciar a *Wallet* pela primeira vez (Figura 5.10) esta gera as chaves criptográficas do utilizador e armazena-as. Seguidamente, a aplicação inicializa a certificação da chave pública do utilizador junto de uma CAP, através do *browser* Web (Figura 5.11).

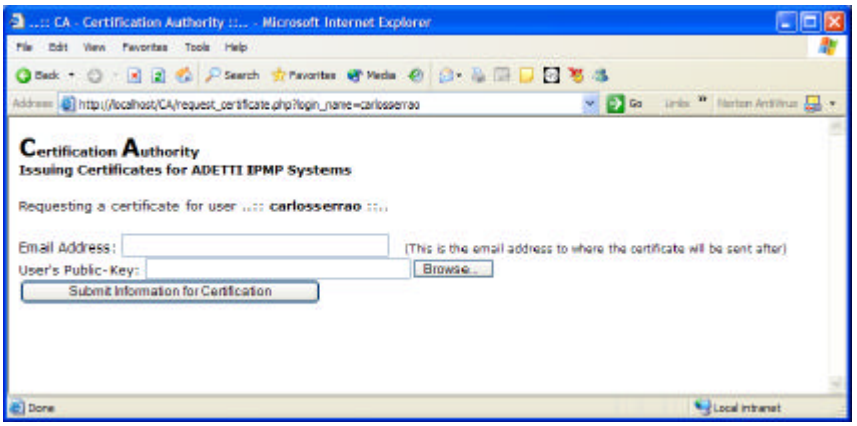


Figura 5.10 Certificação do dados do utilizador

No *site* da CAP o utilizador fornece a sua chave pública em conjunto com mais alguns dos seus dados. O seu endereço de correio electrónico é utilizado para validação e para lhe enviar mais tarde o seu certificado digital emitido pela CAP. Este certificado permitirá que o utilizador se possa registar junto de uma FIP[44] para posteriormente utilizar o sistema.

5.2.3.4 Inscrição do utilizador junto de uma Instituição Financeira

Após estar devidamente credenciado junto de uma CAP, o utilizador regista-se junto de uma FIP.

[44] Plataforma da Instituição Financeira

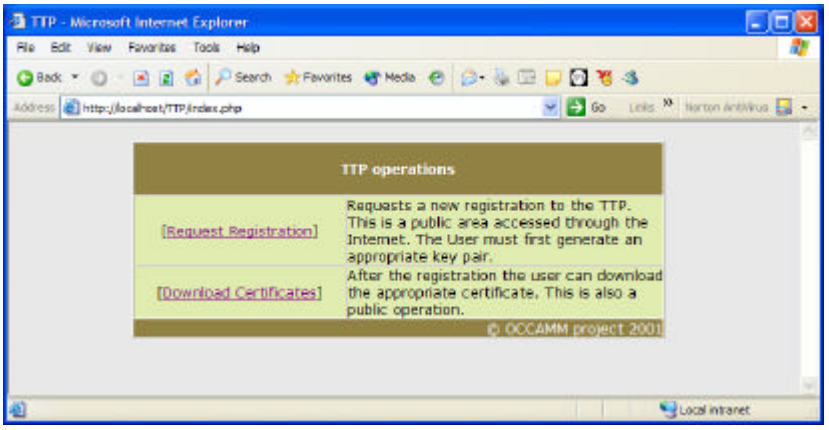


Figura 5.11 Início do processo de registo numa FIP

Após a reinicialização da *Wallet*, esta verifica a existência de uma credencial obtida da CAP e redirecciona o utilizador (*browser* de Web) automaticamente para o *site* de Web da FIP que lhe permite efectuar o registo (Figura 5.12).

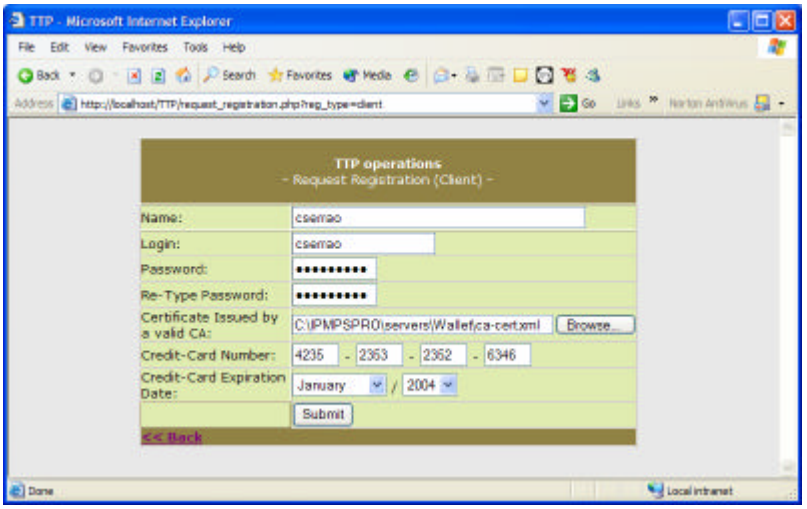


Figura 5.12 Introdução dos dados de registo

O utilizador é solicitado a fornecer uma série de informação relacionada com o meio de pagamento que irá ser utilizado para proceder ao pagamento do conteúdo que pretende adquirir através do sistema OpenSDRM. O utilizador fornece igualmente o certificado obtido a partir da CAP (Figura 5.13).

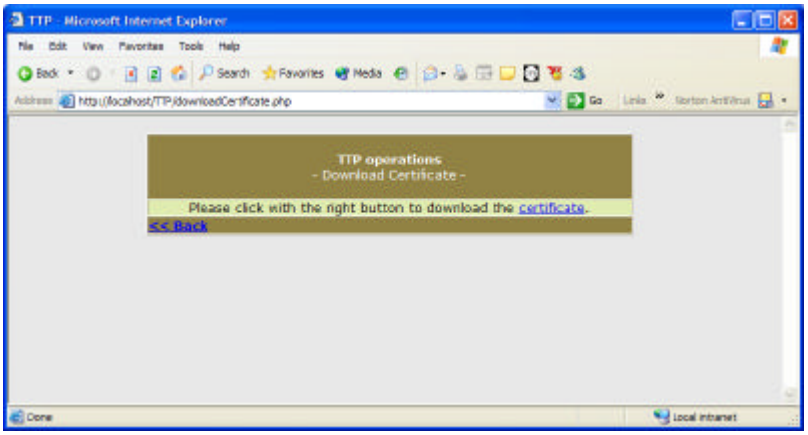


Figura 5.13 Obtenção do certificado na FIP

Após a verificação e validação de todos os dados fornecidos pelo utilizador, o *site* de Web da FIP regista o utilizador e emite um certificado que será posteriormente utilizado pelo utilizador para se registar junto da ECP (Figura 5.14). Esta é a prova de validade de um utilizador, que garante a confiança necessária para uma ECP (conforme havia sido especificado no Capítulo 4).

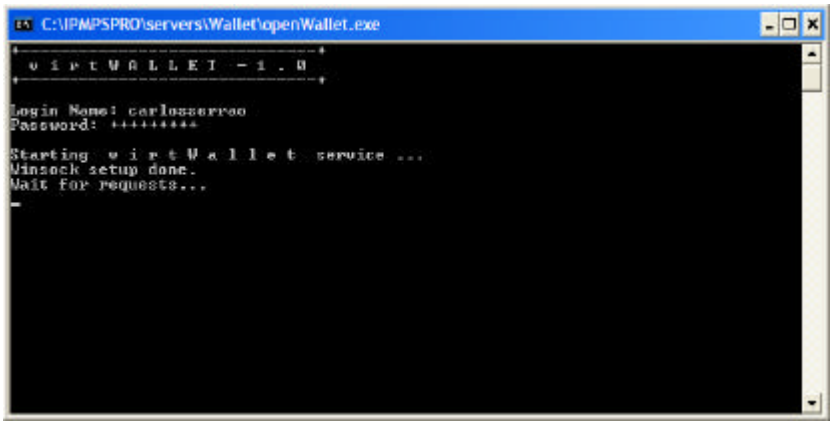


Figura 5.14 *Wallet* em funcionamento

Após a conclusão deste processo a aplicação *Wallet* ficará pronta a receber pedidos de autenticação por parte das aplicações instaladas na OVM do cliente, permitindo que este efectue pagamentos em segurança, usando o meio de pagamento seleccionado (Figura 5.15).

5.2.3.5 Obtenção de Informação

Para adquirir conteúdo digital, o utilizador inicia o seu *browser* Web e liga-se ao *site* Web da ECP OCCAMM para comercialização de música digital. Visualiza então a página principal que proporciona informação acerca do serviço (termos, condições, requisitos, suporte, etc.), assim como instrui o utilizador dos passos necessários para a inscrição do mesmo nesta loja electrónica.

5.2.3.6 Entrada no *site* Web

No *site* da ECP [OCEPPS00], o utilizador selecciona uma ligação para aceder ao catálogo dos produtos e serviços. É apresentado um formulário ao utilizador solicitando a sua autenticação. O utilizador deverá introduzir a sua identificação que fora obtida após um processo de registo bem sucedido, assim como a sua

identificação única de utilizador. No caso do utilizador ainda não estar registado na ECP, deverá então proceder ao seu registo. Durante este processo de registo, o utilizador deverá fornecer o certificado obtido junto da FIP.

Como havia sido referido no capítulo anterior (Capítulo 4, referente ao sistema IPMP desenvolvido) o utilizador necessita obter uma série de credenciais de CAPs válidas e conhecidas do sistema para poder registar-se com sucesso na ECP utilizando o sistema OpenSDRM. Para proceder com sucesso ao registo na ECP, o utilizador teve anteriormente que efectuar o registo numa FIP válida (ver secção 5.4.3.4). Este registo permite que o utilizador forneça à ECP as garantias necessárias de pagamento, estabelecendo um laço de confiança entre ambos.

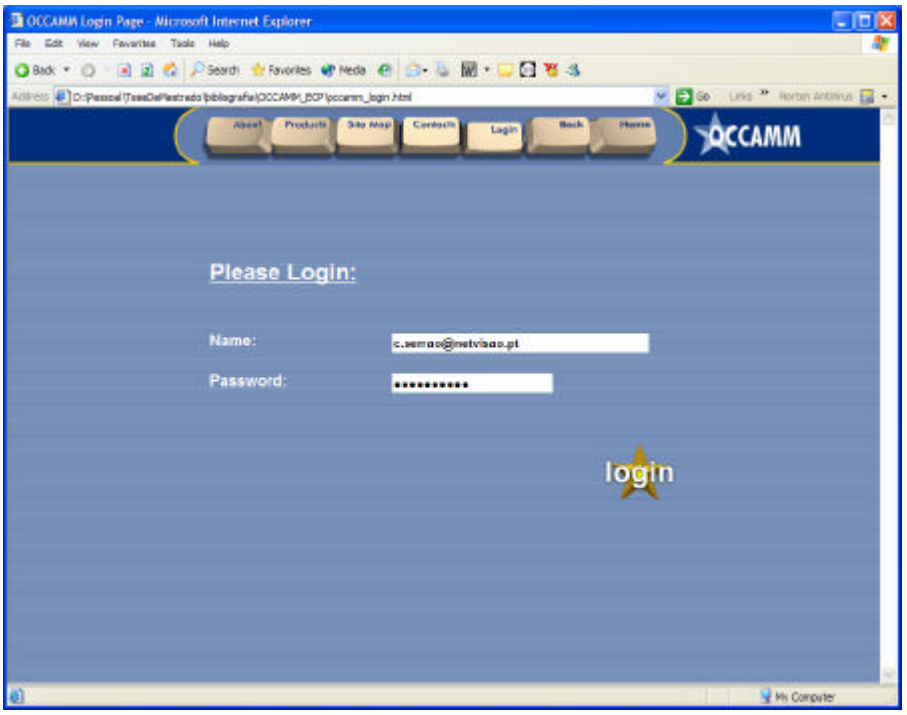


Figura 5.15 Entrada no *site* de música

Após o registo bem sucedido (Figura 5.16) o utilizador estará em condições de poder adquirir e consumir conteúdo disponibilizado no *site* (quer se trate de conteúdo que será descarregado ou fornecido em fluxo contínuo).

5.2.3.7 Consulta do catálogo de Produtos e Serviços

O utilizador pode navegar no catálogo da ECP visualizando a lista de ficheiros de música que se encontram disponíveis na mesma [OCECPS00]. A cada um dos diversos ficheiros de música encontra-se associado um conjunto de várias hiper-ligações que o utilizador poderá escolher (Figura 5.24):

- Previsão da Música: proporciona o descarregamento de um ficheiro que permite somente a previsão da música final (este ficheiro poderá inclusive ser o mesmo que o final, no entanto o utilizador apenas terá acesso a parte do conteúdo e não ao conteúdo total, que apenas estará completamente acessível após a obtenção de uma licença adequada);

- Descarregar Música: esta opção permite que o utilizador possa descarregar o ficheiro da música em formato MP4. Esta opção tem como resultado a criação de uma licença no Servidor de Licenças e uma ordem de envio do conteúdo escolhido através da ligação escolhida pelo utilizador;

Figura 5.16 *Site* Web da loja da ECP: Escolha de Música

5.2.3.8 Descarregamento de um ficheiro MP4

Sempre que o utilizador deseja descarregar um ficheiro de música deve escolher a correspondente hiper-ligação para efectuar esta operação. É apresentada uma nova página ao utilizador em que este deve escolher as condições de licenciamento da música seleccionada. Existem diversas opções disponíveis que incluem desde o número de vezes que se deseja ouvir a música, até ao número de cópias da música que podem ser realizadas (podem ser adicionadas mais opções de licenciamento). O preço final da música é calculado através das escolhas que foram seleccionadas pelo utilizador, que foram sendo acrescentadas ao preço base da mesma. Após o utilizador ter escolhido as condições e o preço ter sido estabelecido e acordado, a ECP assinala o Servidor Multimédia que um determinado ficheiro MP4 deve ser entregue a um utilizador de uma determinada forma (descarregamento, fluxo contínuo).

5.2.3.9 Criação da Licença no Servidor de Licenças

Em termos de arquitectura, o Servidor de Licenças é igualmente um *peer* OPIMA. Este Servidor de Licenças recebe um pedido autenticado da ECP e gera uma licença para o utilizador e conteúdos seleccionados. O formato desta licença é especificado em XML e fica armazenado (de forma segura) na Base de Dados do Servidor de Licenças.

As diferentes condições de licenciamento adoptadas para este teste de utilização real são as seguintes:

Condição	Significado
usage_r_play	Esta condição indica o número de vezes que determinada música poderá ser escutada pelo utilizador que adquiriu a licença em causa. Caso o valor seja igual a '-1' indica que a música poderá ser escutada um número indeterminado de vezes.
usage_r_copies	Esta condição indica o número de cópias que podem ser efectuadas da música em questão pelo utilizador que adquiriu esta licença. No caso do valor ser igual a '-1' indica que a música poderá ser copiada um número indeterminado de vezes.

Outras condições de licenciamento podem ser igualmente utilizadas:

device_type	Esta condição permite especificar em que tipo de dispositivos é que o conteúdo poderá ser mostrado.
expire_date	Esta condição da licença pode especificar uma data em que a licença para desfrutar de um determinado conteúdo irá expirar.
duration_time	Permite especificar qual o tempo de duração da licença, durante a qual o conteúdo poderá ser utilizado.
player_location	Permite indicar em que localização geográfica é que o conteúdo poderá ser utilizado.

5.2.3.10 Descarregar um sistema IPMP

Para visualizar o conteúdo adquirido na ECP, o utilizador utiliza a aplicação cliente OCCAMM apropriada a funcionar sobre uma OVM (Figura 5.18), e tenta abrir o ficheiro MP4 entretanto recebido (Figura 5.19).

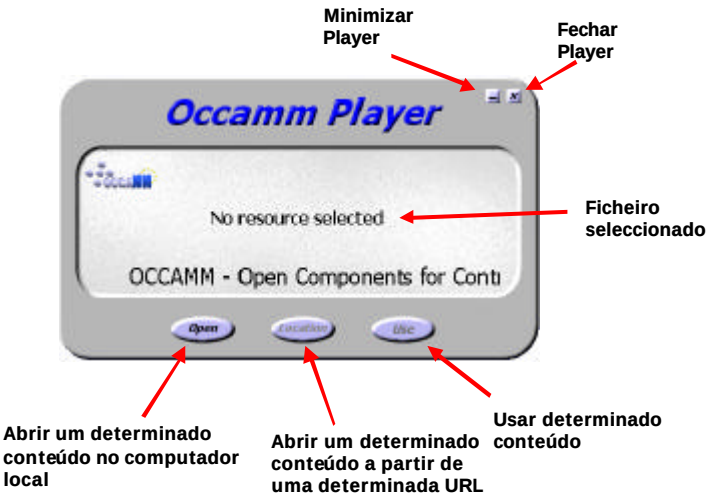


Figura 5.17 A aplicação player de conteúdo

Figura 5.18 Selecção do ficheiro

A OVM lê a estrutura do ficheiro MP4 e, verificando que o mesmo se encontra protegido, apresenta ao utilizador uma lista de sistemas IPMP alternativos que podem ser aplicados ao conteúdo protegido em causa (Figura 5. 20) [OCASAS01, OCIMPATP01].

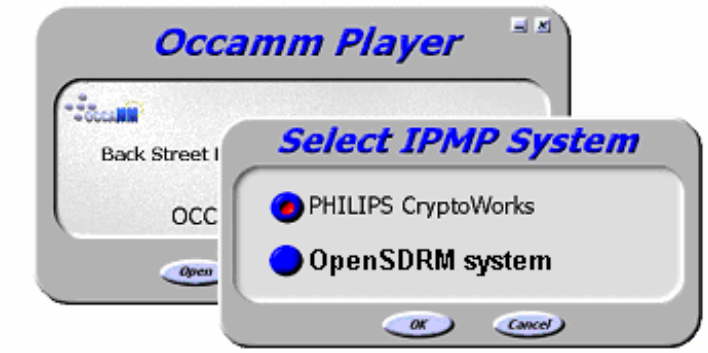


Figura 5.19 Escolha do Sistema IPMP

O utilizador escolhe um dos sistemas IPMP disponíveis. A OVM verifica a existência desse sistema no seu ambiente de execução local e caso não o encontre, efectua o seu descarregamento a partir de um servidor remoto, instalando-o e executando-o em seguida. O descarregamento deste sistema IPMP é realizado a partir de um Servidor de Sistemas IPMP através do OPIMA SAC, obedecendo ao protocolo pré-estabelecido na especificação OPIMA. (conforme o que se encontra especificado no Capítulo 3). Este OPIMA SAC [OPIMASP00] é estabelecido de uma forma segura, recorrendo a autenticação mútua entre a OVM do cliente e o Servidor de Sistemas IPMP, garantindo que o sistema IPMP não irá ser alterado em trânsito por entidades externas.

5.2.3.11 Descarregar a Licença do Servidor de Licenças

Após o estabelecimento das condições de utilização, e da ECP ter solicitado a produção de uma licença ao Servidor de Licenças para o utilizador devidamente autenticado, esta é criada e armazenada para posterior descarregamento.

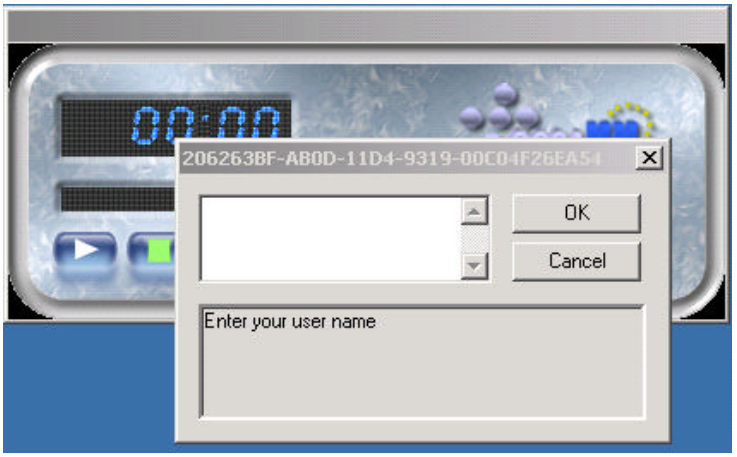


Figura 5.20 Pedido de autenticação do utilizador

Quando a OVM do cliente inicializa o sistema IPMP, este identifica o conteúdo e solicita a autenticação do utilizador para poder aceder aos dados da *Wallet* (Figura 5.21). De seguida, estabelece uma ligação, utilizando o OPIMA SAC com o Servidor de Licenças (esta ligação apenas é estabelecida se se verificar que no sistema do utilizador não existe nenhuma licença válida para o conteúdo em causa). Após uma autenticação válida do utilizador, este indica ao Servidor de Licenças qual o conteúdo para o qual deseja obter a licença de utilização e descarrega-a em segurança. Esta licença contém a chave criptográfica que garante o correcto acesso à visualização do conteúdo, pelo que deve ser descarregada em segurança.

5.2.3.12 Mostrar o conteúdo do ficheiro MP4

O utilizador, após a OVM cliente ter conseguido obter a licença de utilização necessária para usar o conteúdo, utiliza a aplicação OCCAMM para mostrá-lo. Esta aplicação contém diversos botões (*Play*, *Pause*, *Stop*, entre outros) que permitem que o utilizador possa controlar o consumo do conteúdo (Figura 5.22).

Figura 5.21 Visualização do conteúdo

De cada vez que o conteúdo é mostrado, o cliente pede à OVM que desencripte o conteúdo (neste caso, os *Elementary Stream* de áudio e de imagem JPEG) utilizando os parâmetros contidos no sistema IPMP e na chave secreta (AES) contida na licença. De igual forma, a marca de água é extraída e analisada pelo sistema IPMP, que informa o utilizador que a música que está a ser tocada é legítima. Através da leitura da informação de controlo de cópias contida na licença, o sistema IPMP informa igualmente o utilizador de quantas cópias poderá realizar do conteúdo que adquiriu.

5.2.3.13 Obter outra licença

Quando o utilizador tenta escutar a música mais uma vez (depois de ter ultrapassado o número permitido pela licença), o sistema IPMP informa o utilizador que a licença adquirida expirou. O utilizador deve então adquirir uma nova licença para o conteúdo em causa, caso deseje continuar a usufruir do mesmo, repetindo-se o processo de negociação da licença (ver secção 5.4.3.9) e descarregamento da mesma (ver secção 5.4.3.11).

5.3 Metodologia de Avaliação

Aquando da realização dos testes, foi necessária a recolha de alguma informação junto dos utilizadores dos mesmos, de forma a avaliar quais os principais aspectos a melhorarem. Esta secção descreve a forma na qual a informação foi recolhida, acerca da realização dos testes de utilização real de aquisição de música digital.

De forma a poder recolher alguma informação estatística dos utilizadores, foram realizados alguns questionários para que estes pudessem expressar as suas opiniões (estes questionários podem ser encontrados no Anexo E). Estas opiniões foram avaliadas em termos quantitativos e qualitativos, tendo permitido a recolha de sugestões para futuros melhoramentos.

5.4 Resultados e Conclusões

Os testes de utilização real decorreram em paralelo com a colaboração de vários dos parceiros internacionais, no âmbito do projecto OCCAMM [OCPHB00, OCTRADR02]. Assim, a configuração destes testes foi a seguinte:

- ECP e Servidor de Conteúdo: Reino Unido;
- Plataforma de Segurança/OpenSDRM (CAP, Servidor de Licenças, Servidor de Sistemas IPMP e FIP): Portugal;
- Produção de Conteúdo: Itália.

Estes testes decorreram ao longo de cerca de 2 meses e contaram com a presença de vários utilizadores genéricos e alguns utilizadores específicos do sector da música (responsáveis de editoras discográficas e músicos). Foram cerca de 100 utilizadores os que participaram nos testes com a seguinte distribuição/perfil:

- 40 eram fãs de música e estavam interessados nos testes;
- 20 eram utilizadores com pouca experiência na Internet;
- 40 eram utilizadores com muita experiência na Internet;
- 75 tinham já usado outros sistemas de descarregamento de música na Internet;
- 30 já tinham realizado alguma aquisição na Internet;
- 10 tinham já experiência na aquisição de música em *sites* de Internet.

Alguns dos comentários tecidos por parte dos utilizadores, foram os seguintes:

- O *site* da loja de música era fácil de utilizar;
- A aplicação cliente que permitia escutar a música era, por vezes, demasiado lenta a responder às ordens do utilizador e o processo de obtenção de licenças era moroso;
- A qualidade da música disponível no *site* de Web era considerada muito boa, mas a quantidade e variedade da mesma não era muito grande;
- A entrega do conteúdo através da Internet era boa e rápida;
- A aplicação cliente que permitia escutar a música carece de funcionalidades hoje oferecidas por aplicações semelhantes (*Microsoft Media Player*), tais como a possibilidade de criação e utilização de listas de música;
- Por vezes era impossível escutar as músicas, pelo facto de não ser possível efectuar o descarregamento de licenças por indisponibilidade do servidor de licenças;
- O processo de certificação e de registo na FIP torna o processo de subscrição bastante complexo;
- O facto de ser necessária a instalação adicional de *software* no PC dos utilizadores, nomeadamente a *Wallet*, dificulta a utilização do sistema;
- No entanto, a percepção global dos utilizadores era a de que o sistema era seguro [OCTRADR02].

Ao longo deste capítulo foi descrito um dos testes realizados pelo projecto OCCAMM que utilizou o sistema OpenSDRM em conjunto com o sistema IPMP baseado na *Wallet* desenvolvidos no âmbito da presente dissertação. Este teste esteve em funcionamento ao longo de dois meses e contou com a colaboração de vários utilizadores de diversas partes da Europa.

O sistema desenvolvido esteve em funcionamento em paralelo com os testes do projecto OCCAMM, sendo que os dois sistemas IPMP eram perfeitamente interoperáveis entre si.

Em termos globais os testes de utilização real de música foram bem sucedidos e toda a infra-estrutura e *software* desenvolvido foi considerado como fiável e seguro. Genericamente, o conceito de aquisição de licenças *on-line* parece ser comercialmente viável (dependendo do preço a pagar pelas mesmas), no entanto, o sistema de licenças utilizado, torna o processo de utilização de conteúdo demasiadamente dependente da disponibilidade do mesmo. Deveria ser dada uma maior ênfase na utilização e apresentação do sistema, o que permitiria que os utilizadores tivessem uma maior facilidade na utilização do mesmo.

6 CONCLUSÃO

A comercialização de conteúdos através da utilização dos novos formatos e meios de distribuição digitais introduz uma série de questões que nunca antes se haviam colocado com tanta veemência como agora no que concerne à gestão e protecção da propriedade intelectual [STDM01].

A indústria de conteúdos enfrenta hoje um dilema interessante: se por um lado a evolução técnica dos novos formatos e dos canais de distribuição proporcionam excelentes oportunidades de negócio, por outro funcionam como um impulsionador para o desenvolvimento e proliferação da pirataria. Para além disso, a forma como os conteúdos digitais são utilizados nos nossos dias criaram especificidades cada vez mais complexas que apenas podem ser resolvidas, em parte [PDAICE00], recorrendo a soluções técnicas adequadas [TVOC00].

Apesar de diversos estudos realizados demonstrarem que este dilema não pode ser resolvido recorrendo exclusivamente a medidas tecnológicas [PDAICE00], a verdade é que a utilização de soluções integradas que permitam efectuar uma gestão e protecção eficaz dos direitos de autor resolvem uma parte importante deste dilema [TVOC00]. Estas soluções designam-se por DRM – *Digital Rights Management* – (conforme exposto nos Capítulos 3 e 4) e permitem a gestão integrada da propriedade intelectual dos conteúdos digitais.

A gestão destes direitos de autor é extremamente complexa, colocando inúmeras questões a diversos níveis (Figura 6.1). Questões como o formato de representação do conteúdo, identificação única e registo, formatos de meta-informação, linguagens de expressão de direitos ou identificação de utilizadores focam apenas alguns dos pontos a considerar na complexidade da gestão dos direitos de autor de conteúdos digitais [ODRM00]. Estes foram alguns dos aspectos que o sistema OpenSDRM procurou dar resposta.

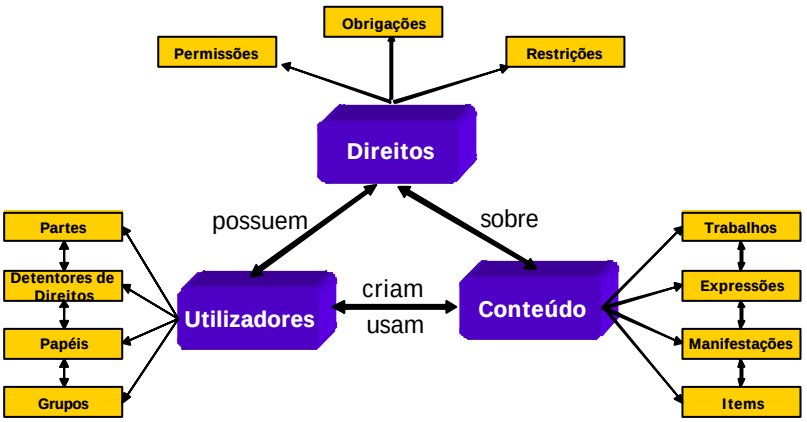


Figura 6.1 A complexidade da gestão dos direitos de autor [ODRM00]

Vários organismos a nível internacional têm-se debruçado sobre a problemática da gestão dos direitos de autor dos conteúdos digitais. Particularmente activos nesta área há a destacar o trabalho dos comités JPEG

e MPEG, embora existam outros de menor dimensão que são igualmente importantes (OCTALIS, TALISMAN[45], OPIMA, OCCAMM, entre outros). No caso do JPEG, e em especial o caso do novo formato JPEG2000 para imagens digitais [JPG2000BK], salienta-se que uma das partes fundamentais da especificação [WG1N2548] dedica uma atenção especial à protecção e gestão do conteúdo digital [WG1N2650]. No MPEG, existem duas vertentes importantes na área da protecção dos direitos de autor: a norma MPEG-4 *IPMP Extensions* e o trabalho do MPEG-21, mais abrangente na definição de medidas de protecção e gestão dos direitos de autor [STDMB02]. Existem ainda empresas que comercializam soluções proprietárias, baseadas em produtos de DRM específicos que desempenham actividades nesta área da gestão e protecção de conteúdos digitais (*Adobe Systems*, *Content Guard Holdings*, *InterTrust Technologies*, *Microsoft*). É, no entanto, importante não apenas precaver os direitos de autor, mas criar igualmente soluções abertas (por oposição às proprietárias) que permitam a universalização do conceito e que vários fornecedores e clientes possam partilhar informação, em respeito pelas leis instituídas e independentemente das soluções tecnológicas que lhes sejam subjacentes.

Apesar das soluções DRM serem bastante extensas em termos de funcionalidades e de suportarem aspectos como a descrição, identificação, comércio, protecção, monitorização e acompanhamento de todas as formas de direitos de utilização de bens tangíveis e intangíveis, estas sempre tiveram um ênfase muito forte na dicotomia "segurança/protecção" pela imposição dos direitos digitais sobre determinado conteúdo [IDRM02]. As PKI desempenham por isso um papel importante nas soluções DRM do futuro. Estas tecnologias permitem responder a alguns dos requisitos/funcionalidades que foram identificadas para os DRM que são apenas resolvidas através da integração de ambas [UDRMS01, STDM01].

No sistema OpenSDRM que foi implementado (ver Capítulo 4 e Anexo H), as PKI desempenham um papel importante no estabelecimento de relações de confiança entre entidades distintas, através da garantia de princípios base como a Autenticação, Privacidade, Integridade e o Não-repúdio. Estas relações de confiança são imprescindíveis para a gestão dos direitos de autor num cenário de comercialização electrónica de conteúdos digitais [ECRTBD00]. O autor do conteúdo necessita de confiar no sistema de comercialização para salvaguarda dos seus direitos, assim como o utilizador final precisa de confiar de igual forma no sistema de comercialização por forma a garantir que o pagamento efectuado é válido e que o conteúdo recebido é original e corresponde exactamente ao solicitado. O OpenSDRM integra as funcionalidades de uma solução DRM, em parte, desenvolvida no âmbito da especificação OPIMA e do projecto Europeu OCCAMM, com as funcionalidades PKI necessárias, de forma a criar os mecanismos necessários para o Comércio Electrónico seguro de conteúdos digitais.

Este sistema permitiu dar uma resposta a questões que eram colocadas na anterior solução DRM, nomeadamente garantir:

- A identificação e autenticação dos diversos intervenientes na negociação de conteúdo digital (comerciante, utilizador final);
- A segurança e a integridade dos dados que eram transmitidos entre os diversos sistemas;
- A integridade e confidencialidade do conteúdo digital através da encriptação do mesmo;
- O estabelecimento de confiança entre o comprador e o vendedor de conteúdos digitais;

[45] TALISMAN - Tracing Authors'rights by Labelling Image Services and Monitoring Access Network (ACTS AC019)

- O estabelecimento de relações seguras com serviços financeiros de forma a garantir o pagamento do conteúdo consumido;
- A gestão das licenças de utilização do conteúdo assim como a sua respectiva integridade.

O sistema foi testado e validado através da realização de testes de utilização real em que participaram diversos fornecedores de conteúdo e utilizadores finais. A escolha pela música como forma de conteúdo digital a utilizar foi uma decisão que teve por base o facto de se tratar de um conteúdo com bastante popularidade na Internet e que é o alvo preferencial da pirataria. A escolha pelo formato MPEG-4 permitiu utilizar tecnologias de criação de conteúdo já existentes, permitindo adicionar valor à música pela integração de outros tipos de conteúdo (nomeadamente imagens digitais contendo imagens da banda a que se referia a música). Os resultados dos testes (ver Capítulo 5) reflectem que apesar do sistema garantir a protecção do conteúdo são ainda necessários melhoramentos ao nível da facilidade de utilização (segurança versus facilidade de utilização), com vista a melhorar a sua aceitação pelos utilizadores do sistema.

Este trabalho apresenta algumas soluções em termos da utilização das soluções DRM em conjunto com as PKI, nomeadamente na integração de sistemas de certificação digital X.509 e dos novos formatos especificados pelo W3C em XML. Requer, contudo, uma integração mais profunda entre ambos em concordância com as novas normas de entidades de normalização internacionais, nomeadamente o MPEG. De facto, o acompanhamento e evolução destas normas e a sua integração com o sistema OpenSDRM poderão constituir o catalizador para a continuação deste trabalho, que pelas possibilidades que apresenta, demonstra possuir as características adequadas para projectos futuros.

Acrescente-se ainda, que uma parte substancial do trabalho de concepção e implementação aqui apresentado foi integrado na auditoria técnica realizada ao projecto OCCAMM em Dezembro de 2001, tendo recebido (no global do projecto) uma apreciação bastante positiva por parte dos auditores.

Espero que este trabalho possa contribuir de certa forma para uma integração mais facilitada dos dois sistemas assim como para impulsionar o desenvolvimento de novos sistemas de comercialização electrónica segura de conteúdos digitais.

REFERÊNCIAS BIBLIOGRÁFICAS

[AESPRIJ99] Daemen J., Rijmen, V., "AES Proposal: Rijndael, AES Proposal", 1999

[AHVCERT00] Goodenough, D., "An Heretic's view of certificates", David Goodenough & Associates Limited, http://www.dga.ca.uk, 2000

[AIAAD00] Myrvang, H., "An Infrastructure for Authentication, Authorization and Delegation", Faculty of Science, University of Tromso, 2000

[APKI99] The Open Group, "Architecture for Public Key Infrastructures (APKI)", Open Group, 1999

[ASN1XML02] Mas, J., Orri, X., "ASN.1 versus XML", Octalis SA., http://www.octalis.com, 2002

[AVTRELRIS97] Bohm, N., "Authentication, reliability and Risks", Meta Certificate Group, http://www.mcg.org.br, 1997

[BEC01] CommerceNet, "Barriers to Electronic Commerce - 2000 Study", 2000

[CATKEC00] Eng, T., "Certificate Authorities: The keys to E-Commerce?", PlanetIT, http://www.planetit.com, 2000

[CCSS99] Stevenson, F., "Cryptanalysis of Contents Scrambling System", http://www.lemuria.org/DeCSS/crypto.gp.nu/ , 1999

[CEICOM97] Gerck, E., "Certification: Extrinsic, Intrinsic and Combined", Meta Certificate Group, http://www.mcg.org.br, 1997

[CENI99] Silva, M., Silva, A., Romão, A., Conde, N., "Comércio Electrónico na Internet", FCA, 1999

[CP2PB2B00] White, A., "Convergence of P2P and B2B: New Economy Business Models", Logility, Inc., 2000

[CPYGMSW01 Guterman, J., "Click and Play: Your Guide to Music *Sites* on the Web", Business2, http://www.business2.com, 2001

[CSSSEC00] Kahaner, L., "Companies strive for Simpler Security", Information Week Online, http://www.informationweek.com, 2000

[DMPP01] Fisher, W., "Digital Music: Problems and Possibilities", http://www.law.harvard.edu, 2001

[DPCC97] Certisign, "Declaração das Práticas de Certificação da Certisign - Versão 1.0", Certisign, http://www.certisign.com.br, 1997

[DRBSA02] "Digital Rights: Background, Systems, Assessment", Commission Staff Working Draft, Commision of the European Communities, 2002

[EBETNREM00] Norris, M., West, S., Gaughan, K., “eBusiness Essentials: Technology and Network Requirements for the Electronic Marketplace”, John Wiley & Sons, 2000

[EBMOC99] Rao, B., “Emerging Business Models in Online Commerce - version 1.0”, 1999

[ECRTBD00] Keen, P., Ballance, C., Chan, S., Schrume, S., “Electronic Commerce Relationships: Trust By Design”, Prentice Hall PTR, 2000

[EXMLS01] Mactaggart, M., “Enabling XML security - An introduction to XML encryption and XML signature”, IBM, 2001

[ICAPKC96] Halsey, B., “An Introduction To Certification Authorities and Public Key Cryptography”, Argorne National Laboratory, http://www.anl.gov, 1996

[IDCWH98] Rundreen, A., “ID Certificates - Why and How”, 1998

[IDRM02] Franklin, S., “Integrating DRM”, new.architect magazine, http://www.newarchitectmag.com, 2002

[IGSAV99] Larson, A., “Inquérito global sobre segurança - Ataques de vírus”, Internet World, 1999

[IMHONISSR99] Meritt, J., “IMHO: New IS Security Requisites”, Information Week Online, 1999

[IPMF00] Chiariglione, L., “Intellectual Property in the Multimedia Framework”, Management of Digital Rights, Berlin, 2000

[JPG2000BK] Taubman, D., Marcellin, M., "JPEG2000: Image Compression: Fundamentals, Standards and Practice", Kluwer Academic Publishers, 2001

[KBMP3AAC] Brandenburg, K., “MP3 and AAC explained”, AES 17th. International Conference on High Quality Audio Coding, Fraunhofer Institute for Integrated Circuits, 1999, http://www.ece.cmu.edu/~ee545/MP3/docs/mp3_explained.pdf

[MP3BMD00] Merck A. “MP3.com - business model and development”, MEBIS, 2000

[MPEGA00] Chiariglione, L., “MPEG and Audio”, Grammy 2000, July 2000

[MPKI96] Maurer, U., “Modelling a Public-Key Infrastructure”, European Symposium on Research in Computer Security (ESORICS'96), Lecture Notes in Computer Science, Berlin: Springer-Verlag, vol. 1146, pp. 325-350, 1996

[NAICPGP00] Network Associates, “Introduction to Cryptography”, PGP 7.0, Network Associates Inc., Setembro 2000

[NEMD01] Haes, J., Hummel, J., “Napster and the Economics of Music Distribution”, NetAcademy, http://www.netacademy.org, 2001

[NSEAS00] Stallings, W., “Networking Security Essentials: Applications and Standards”, Prentice Hall, 2000

[OCASASFD00]

[OCBMS00] OCCAMM Project, “Business Model Selection”, D3, WP1, IST-11443, 2000

[OCCSTOP00] OCCAMM Project, "Cryptographic/scrambling tools and OPIMA protocols functional description", D10, WP3, IST-11443, 2000

[OCECPS00] OCCAMM Project, "E-Commerce Platform Specification", D16, WP5, IST-11443, 2000

[OCFDOVM00] OCCAMM Project, "Functional Description of the OPIMA Virtual Machine", D7, WP3, IST-11443, 2000

[OCIMPATP01] OCCAMM Project, "Interactive Multimedia Player & Authoring Tool Platform", D18, WP6, IST-11443, 2001

[OCIOSF01] OCCAMM Project, "Integrated OCCAMM System Facility", D23, WP5, IST-11443, 2001

[OCISAFD00] OCCAMM Project, "IPMP System API Functional Description", D8, WP3, IST-11443, 2000

[OCOLSMD00] OCCAMM Project, "OnLine Secure Music Distribution", D5, WP1, IST-11443, 2000

[OCOOSS01] OCCAMM Project, "Overall OCCAMM System Specification", D24, WP2, IST-11443, 2001

[OCPH00] OCCAMM Project, "Project Handbook", D2, WP8, IST-11443, 2000

[OCSAS01] OCCAMM Project, "Sample Application Software", D22, WP6, IST-11443, 2001

[OCSX509CA98] Gerk, E., "Overview of Certification Systems: X.509, CA, PGP, and SPKI", http://www.mcg.org.br, 1998

[OCTRADR02] OCCAMM Project, "Trial Report, Achievements, Difficulties, Recommendations for Subsequent Exploitation", D37, WP7, IST-11443, 2001

[ODRLSP01] Iannela, R., "Open Digital Rights Language (ODRL) – Version 1.0", ODRL, http://www.odrl.net, 2001

[ODRM00] Iannella, R., "Open Digital Rights Management", Position Paper to W3C DRM Workshop, IPR Systems, Lda., 2000

[OFPKI00] Hulmic, G., "Options for Public Key Infrastructure", Information Week Online, http://www.informationweek.com, 2000

[OMPEG4S02] Koenen, R., "Overview of the MPEG-4 Standard", ISO/IEC JTC1/SC29/WG11 N4668, MPEG, 2002

[OPIMASP00] OPIMA Charter, "OPIMA specification version 1.1", 2000

[OSPKIB00] Xenitellis, S., "The Open–source PKI Book – A guide to PKIs and Open–source Implementations", OpenCA Group, http://www.openca.org, 2000

[PACS00] Ellison, C., Aura, T., "Privacy and Accountability in Certificate Systems", Helsinki University of Technology Laboratory for Theoretical Computer Science, Research Reports 61, 2000

[PDAICE00] Marques, J., "Protecção de Direitos de Autor e seu Impacto no Comércio Electrónico", Dissertação de Mestrado, ISCTE, 2000

[PKIEG01] Baltimore Technologies, "Public Key Infrastructures - An Evaluation Guide", Baltimore Technologies Whitepaper, 2001

[PKIIF01] Lloyd, S., Brink, D., Nash, A., Buhle, G., Cicovic, N., "PKI Interoperability Framework", PKI Forum, http://www.pkiforum.org, 2001

[PKIIMES01] Nash, A., Duane, W., Joseph, C., Brink, D., "PKI: Implementing and Managing E-Security", Osborne - McGrawHill, 2001

[PKIKSEC01] Railsback, K., "PKI is the key to secure ecommerce", Infoworld, http://www.itworld.com, 2001

[PKIWTB01] Austin, T., "PKI – A Wiley Tech Brief", John Wiley and Sons, 2001

[PPKI01] Housley, R., Polk, T., "Planning for PKI – Best practices guide for deploying Public Key Infrastructure", John Wiley and Sons, 2001

[RFC2401] Kent, S., Atkinson, R., "Security Architecture for the Internet Protocol", RFC2401, http:// http://www.ietf.org/rfc/rfc2401.txt, 1998

[RFC2402] Kent, S., Atkinson, R., "IP Authentication Header", RFC2402, http:// http://www.ietf.org/rfc/rfc2402.txt, 1998

[RFC2406] Kent, S., Atkinson, R., "IP Encapsulating Security Payload (ESP)", RFC2406, http:// http://www.ietf.org/rfc/rfc2406.txt, 1998

[RFC2408] Maughan, D., Schertler, M., Schneider, M., Turner, J., "Internet Security Association and Key Management Protocol (ISAKMP)", RFC2408, http:// http://www.ietf.org/rfc/rfc2408.txt, 1998

[RFC2440] Callas, J., Donnerhacke, L., Finney, H., Thayer, R., "OpenPGP Message Format", RFC2440, http:// http://www.ietf.org/rfc/rfc2440.txt,1998

[RFC2527] Chokhani, S., Ford, W., "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework", RFC2527, http:// http://www.ietf.org/rfc/rfc2527.txt,1999

[RPKIECCA00] Ellison, C., Schneier, B., "Risks of PKI: E-Commerce", Communications of the ACM, Vol. 43, N.2, 2000

[RSALFAQ00] RSA Laboratories, "RSA Labs FAQ - Version 4.1", RSA Laboratories, Inc., 2000

[SDDFT98] Baxter, A., "Standards: Driving down the fast track", Finantial Times, 1998

[SGDD00] Niedermeier, T., "Spectacular Growth for Digital Delivery", e-Gateway, http://www.e-gateway.com, 2000

[SPKC98] Ellison, C., Frantz, B., Lampson, B., Rivest, R., Thomas, B., Ylonen, T., "Simple Public Key Certificate", Internet Draft, 1998

[SPKICT98] Ellison, C., Frantz, B., Lampson, B., Rivest, R., Thomas, B., Ylonen, T., "SPKI Certificate Theory", Internet Draft, 1998

[SPKIREQ98] Ellison, C., "SPKI Requirements", Internet Draft, 1998

[SPKISDSIWT00] Ellison, C., "SPKI/SDSI and the web of trust", http://world.std.com/~cme/html/web.html, 2000

[SPKIXMLCS01] Mas, J., Orri, X., "SPKI- XML Certificate Structure", Internet Draft, 2001

[SSLTLS99] Thomas, S., "SSL and TLS – Securing the Web, John Wiley and Sons, 2000

[STDM01] LEPRÉVOST, F., WARUSFEL, B., "Security Technologies for Digital Media", European Parliament, Directorate-General for Research, Directorate A, STOA Programme, 2001

[STDMB02] Chiariglione, L., "Standard technologies to develop the multimedia business", MPEG-4 Conference, Paris, 2002

[SXMLKPKIS01] Kobrelus, K., "Simplification, not XML is the key to PKI success", Network World, 2001

[TCFMI00] Baker, V., "The Changing Face of the Music Industry", Gartner Group, 1999

[TEPTP02] Edwards, S., "Translating ePublishing to Profitability", Trends Report 2001, Trends Shaping the Digital Economy, SIIA, 2002

[TIMCP97] Gerk, E., "The Intrinsic and Meta-Certification Primer", Meta-Certificate Primer, http://www.mcg.org.br, 1997

[TKPWOLMD01] Kleinschmit, M., "TEMPO: Keeping Pace with Online Music Distribution",IPSOS-REID CORPORATION, http://www.ipsos-reid.com, 2001

[TNYMBK00] Chiariglione, L., "Taming the net? You must be kidding!", XVII World Telecommunication Conference, Birmingham, 2000

[TPKIRRR99] Smart, B., "Trivial Public Key Infrastructure - Rationale, Requirements and Roadmap", http://weever.vic.cmis.au/~smart/tpki.html, 1999

[TRASOTI00] Global Internet Project, "The reliability and security of the Internet", http://www.gip.org, 2000

[TRPKI00] Ellison, C., Schneier, B., "Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure", Computer Security Journal, Volume XVI, Number 1, 2000

[TRWMTRRI98] Gerck, E., "Towards a Real World Model of Trust: Reliance on Received Information", Meta Certificate Group, http://www.mcg.org.br, 1998

[TVOC00] Chiariglione, L., "The value of content", MIT Technology Review, March/April 2000

[UDRMS01] Duhl, J., Kevorkian, S., "Understanding DRM Systems", An IDC White Paper, 2001

[UPKICSDC99] Addams, C., Lloyd, S., "Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations", Mac Millan Technicall Publishing, 1999

[UPKINF99] RSA Data Security, "Understanding Public Key Infrastructures, RSA Data Security Whitepaper", http://www.rsa.com, 1999

[WG1N2548] Conan, V., Rollin, C., "JPSEC Scope and Requirements 2.0", ISO/IEC JTC 1/SC 29/WG1 N2548, 2002

[WG1N2650] Serrão, C., Conan, V., Sadourny, Y., "JPSEC – Protecting the JPEG2000 code-stream", ISO/IEC JTC 1/SC 29/WG1 N2650, 2002

[WICHTIL98] Gerck, E., "Why is certification harder than it looks?", Meta Certificate Group, http://www.mcg.org.br, 1998

[WSCRTS97] Garfinkel, S., Spafford, G., “Web Security & Commerce: Risks, Technologies and Strategies”, O'Reilly & Associates, Inc., 1997

[WSTXMLS01] “Web Services trust and XML Security Standards”, Entrust, 2001

[XMLESPKIC00] Paajuri, J., “XML Encoding of SPKI Certificates”, Internet Draft, 2000

[XMLKMS01] Verisign, Microsoft, webMethods, “XML Key management Specifications (XKMS)”, Draft Version 1.1 draft 4, 2001

[XMLSSP01] Eartlake, D., Reagle, J., Solo, D., “XML - Signature Syntax and Processing”, XML Digital Signature Working Group, Internet Draft, 2001

ANEXO A – GLOSSÁRIO DE TERMOS

Sigla	Significado em Inglês	Significado em Português
A2B	Administration to Business	Administração para Negócio
AES	Advanced Encryption Standard	Norma de Encriptação Avançada
API	Application Program Interface	Interface para Aplicações de Programas
ASCII	American Standard Code for Information Interchange	Código Americano Normalizado para Troca de Informação
ASN.1	Abstract Syntax Notation One	Notação Abstracta de Sintaxe Um
B2B	Business to Business	Negócio para Negócio
B2C	Business to Consumer	Negócio para Consumidor
BER	Basic Encoding Rules	Regras Básicas de Codificação
C2A	Consumer to Administration	Consumidor para Administração
C2B	Consumer to Business	Consumidor para Negócio
C2C	Consumer to Consumer	Consumidor para Consumidor
CA	Certification Authority	Autoridade de Certificação
CD	Compact Disc	Disco Compacto
CRC	Cyclic Redundancy Checking	Verificação Cíclica de Redundância
CRL	Certificate Revocation List	Lista de Revogação de Certificados
DDOS	Distributed Denial of Service	Negação de Serviço Distribuído
DER	Distinguished Encoding Rules	Regras de Codificação Distintas
DES	Data Encryption Standard	Norma de Encriptação de Dados
DN	Distinguished Name	Nome Distinto
DNS	Distributed Name System	Sistema de Nomes Distribuídos
DOM	Document Object Model	Modelo Documental de Objectos
DOS	Denial of Service	Negação de Serviço
DRDOS	Distributed Redirected Denial of Service	Negação de Serviço Distribuído e Redireccionado
DRM	Digital Rights Management	Gestão de Direitos Digitais
DTD	Document Type Definition	Definição de Tipos do Documento
DVD	Digital Versatil Disc	Disco Digital Versátil
ESP	Encapsulating Security Payload	
IEC	International Electrotechnical Commission	Comissão Electrotécnica Internacional
IETF	Internet Engineering Task Force	Força de Trabalho de Engenharia da

		Internet
IKE	Internet Key Exchange	Troca de Chaves via Internet
IPMP	Intelectual Property Management and Protection	Gestão e Protecção da Propriedade Intelectual
ISO	International Standards Organization	Organização Internacional de Normalização
ISP	Internet Service Provider	Fornecedor de Serviços Internet
ITA	Industry Technical Agreement	
ITU-T	Telecommunication Standardization Sector of the International Telecommunications Union	
KDC	Key Distribution Center	Centro Distribuidor de Chaves
LISP	List Processing Language	
MAC	Message Authentication Code	Código de Autenticação de Mensagens
MIME	Multi-Purpose Internet Mail Extensions	
MIT	Massachutess Institute of Technology	Instituto de Tecnologia de Massachutess
MP3	MPEG Layer III	Camada III do MPEG
MPEG	Motion Pictures Expert Group	Grupo de Peritos de Imagens em Movimento
OCCAMM	Open Components for Controlled Access to Multimedia Material	Componentes Abertos para Acesso Controlado a Material Multimédia
OPIMA	Open Platform for Interactive Multimedia Access	Plataforma Aberta para Acesso Interactivo a Multimédia
OVM	OPIMA Virtual Machine	Máquina Virtual OPIMA
P2P	Peer to Peer	
PEM	Privacy Enhanced Mail	
PGP	Pretty Good Privacy	
PIN	Personal Identification Number	Número de Identificação Pessoal
PKCS	Public-Key Cryptographic Standards	Normas de Criptografia de Chave Pública
PKI	Public Key Infrastructure	Infra-estrutura de Chave Pública
PKIX	Public Key Infrastructure X.509	Infra-estrutura de Chave Pública X.509
RA	Registration Authority	Autoridade de Registo
RSA	Rivest, Shamir and Adleman	
S/MIME	Secure MIME	MIME Seguro
SAC	Secure and Authenticated Channel	Canal Autenticado e Seguro
SAML	Security Assertion Markup Language	

SAX	Simple API for XML	
SDSI	Simple Distributed Security Infrastructure	Infra-estrutura de Segurança Simples e Distribuída
SET	Secure Electronic Transactions	Transacções Electrónicas Seguras
SOAP	Simple Object Access Protocol	Protocolo Simples de Acesso a Objectos
SPKI	Simple Public Key Infrastructure	Infra-estrutura de Chave Pública Simples
SSO	Single Sign-On	Processo de autenticação de um utilizador numa sessão que permite que este possa aceder a multiplas aplicações usando uma única autenticação.
UDDI	Universal Description, Discovery and Integration	Descrição, Descoberta e Integração Universal
VPN	Virtual Private Network	Rede Privada Virtual
WS	Web Services	Serviços Web
WSDL	Web Services Description Language	Linguagem de Descrição de Serviços Web
WWW	World Wide Web	
XACL	XML Access Control Language	
XKISS	XML Key Information Service Specification	
XKMS	XML Key Management Specification	
XKRSS	XML Key Registration Service Specification	
XML	Extensible Markup Language	
XMLDSig	XML Digital Signatures	Assinaturas Digitais XML
XMLEnc	XML Encryption	Encriptação XML
XSL	Extensible Stylesheet Language	Linguagem de Definição de Estilos Extensível

ANEXO B – NOTAÇÕES UTILIZADAS

Neste anexo pode ser encontrada a descrição da notação utilizada para descrever o sistema OpenSDRM que se encontra descrito no Capítulo 4 do presente documento.

$Cert_{Ent}^{Tipo}${dados}: representa uma credencial do tipo **Tipo** emitida por uma entidade **Ent** e que certifica os dados **dados**, ou seja **Ent** assina digitalmente a informação **dados** e formata-a segundo **Tipo**;

$Kpub^{Ent}$: representa a chave criptográfica pública de um par de chaves de uma entidade **Ent**;

$Kpriv^{Ent}$: representa a chave criptográfica privada de um par de chaves de uma entidade **Ent**;

K_{ALG}: representa uma chave criptográfica secreta usando o algoritmo **ALG**;

K_{ALG}[dados]: representa a informação dados encriptada com uma chave secreta com o algoritmo **ALG**;

NIB: representa os dados da conta da instituição bancária que irá receber os pagamentos por parte dos diversos utilizadores da ECP;

MP: representa os dados que o utilizador fornece como meio de pagamento. Este sistema pressupõe que qualquer meio de pagamento é válido desde que seja validado por uma FIP;

REQ^{Tipo}{dados}: especifica o pedido de uma licença especificada por **dados** de um determinado **Tipo**;

C_{id}: identificação única de um determinado conteúdo multimédia;

UCP_{id}: identificação única de um determinado utilizador;

LIC[dados]: credencial que representa uma licença que contém informação indicada por **dados**, que são compostos, entre outros por: **UR_{play}**, **UR_{copies}**, **C_{key}** e **Value**;

UR_{play}: condição da licença que representa o número de vezes que um determinado conteúdo pode ser consumido (no caso da música, corresponde ao número de vezes que esta pode ser escutada);

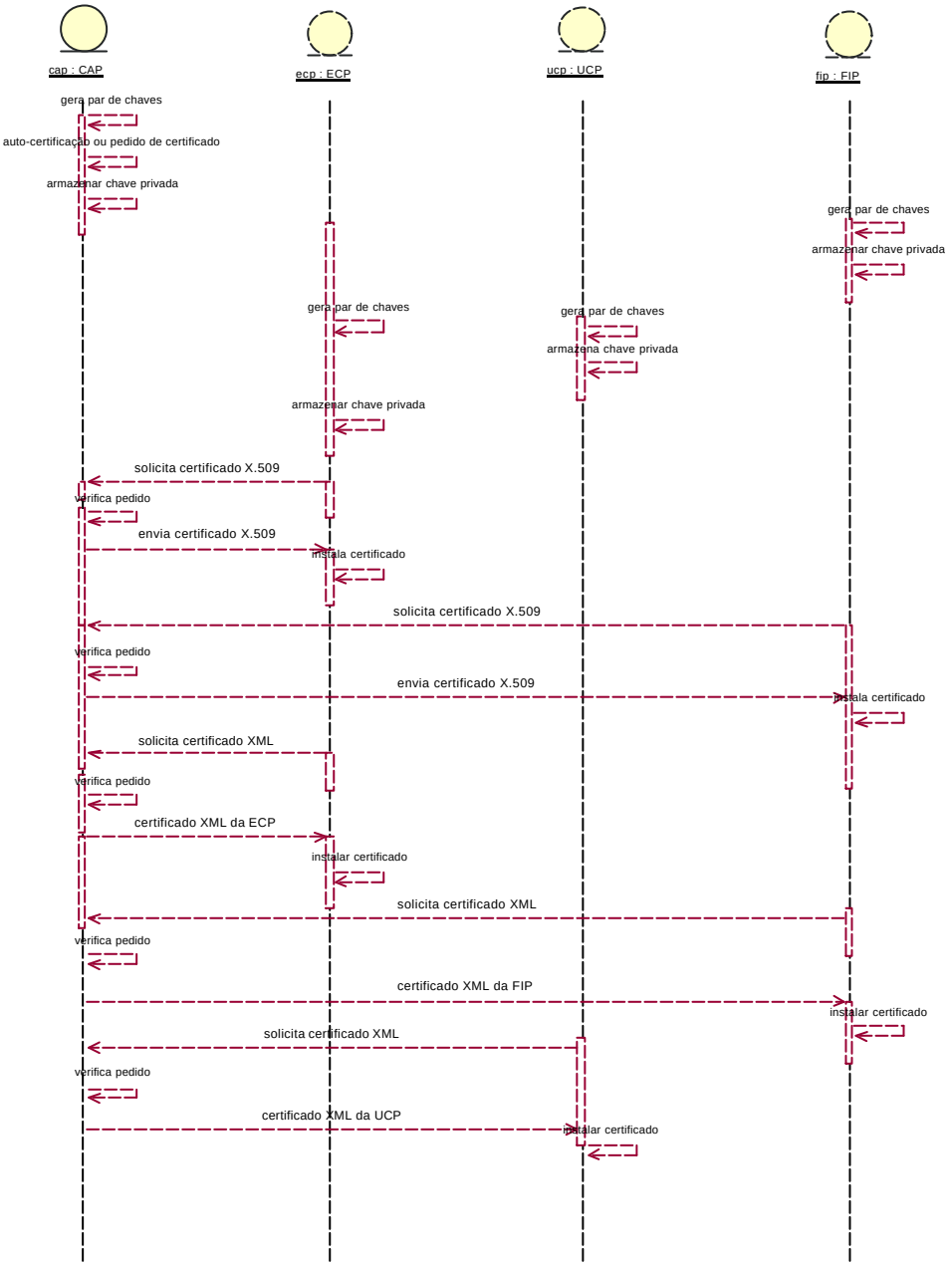
UR_{copies}: condição da licença que representa o número de cópias que pode ser efectuada a um determinado conteúdo;

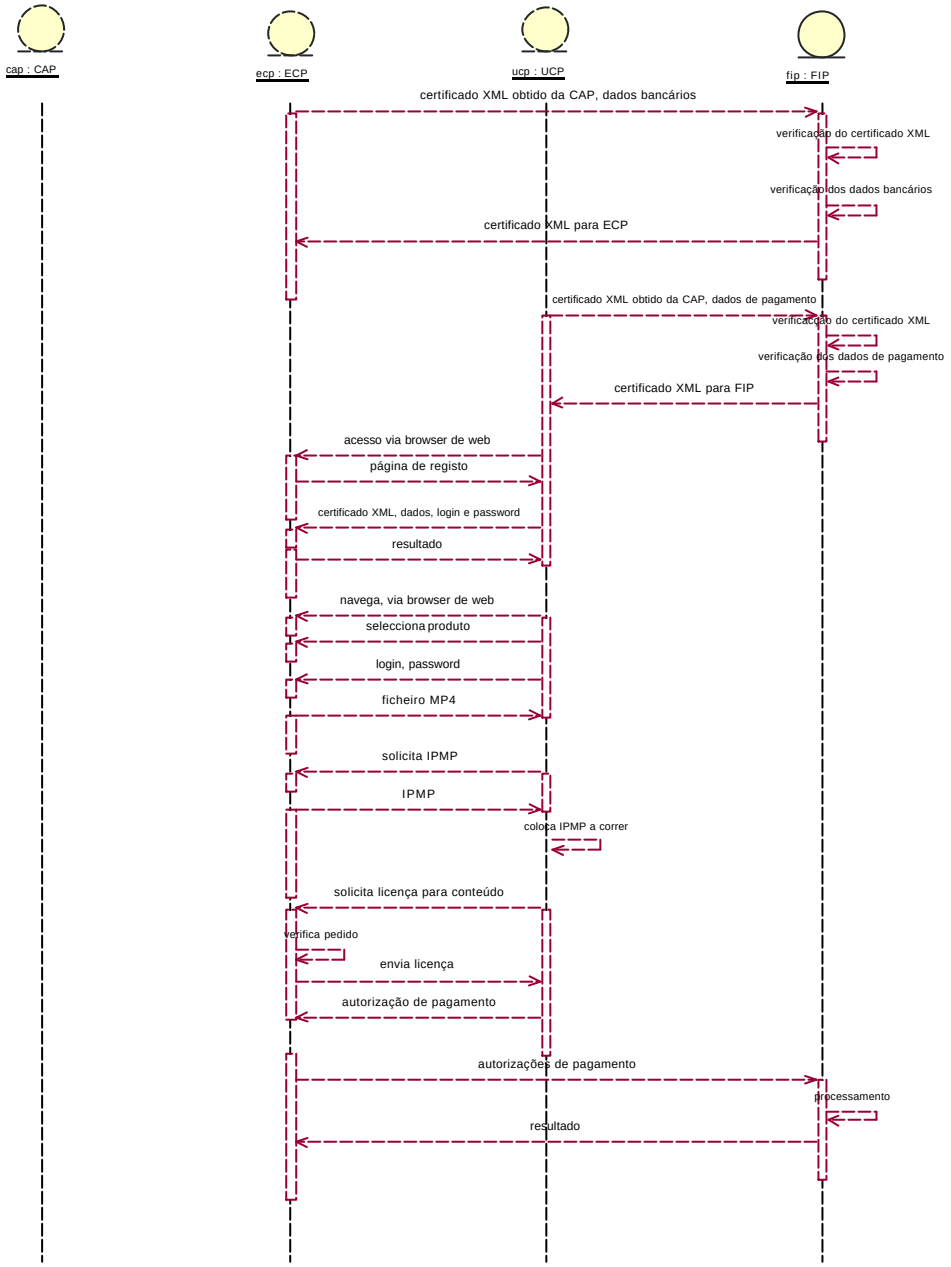
C_{key}: identifica a chave que foi utilizada para encriptar o conteúdo;

Value: identifica o valor que o utilizador terá que pagar para aceder ao conteúdo segundo as condições solicitadas pelo utilizador aquando da aquisição do mesmo;

PAYdata[dados]: representa os dados de pagamento que o utilizador forneceu à ECP para efectuar os pagamentos do conteúdo descarregado da mesma.

ANEXO C – PROTOCOLO DO SISTEMA OPENSDRM




cap : CAP
ecp : ECP
ucp : UCP
fip : FIP
certificado XML obtido da CAP, dados bancários
verificação do certificado XML
verificação dos dados bancários
certificado XML para ECP
certificado XML obtido da CAP, dados de pagamento
verificação do certificado XML
verificação dos dados de pagamento
certificado XML para FIP
acesso via browser de web
página de registo
certificado XML, dados, login e password
resultado
navega, via browser de web
selecciona produto
login, password
ficheiro MP4
solicita IPMP
IPMP
coloca IPMP a correr
solicita licença para conteúdo
verifica pedido
envia licença
autorização de pagamento
autorizações de pagamento
processamento
resultado

ANEXO D – ESQUEMA XML DO SISTEMA OPENSDRM - DTD E XSD

Neste anexo pode ser encontrada a especificação XML completa de todos os certificados e mensagens que são utilizados pelo sistema OpenSDRM que se encontra descrito no Capítulo 4 do presente documento.

Esta especificação utiliza a notação W3C XML DTD e *Schema Definition* (XSD). O XSD encontra-se apresentado de duas formas distintas: uma textual e outra gráfica. Esta notação XSD permite especificar formalmente que elementos e a sua respectiva designação fazem parte de um determinado documento XML, e quais são as suas combinações possíveis. Define igualmente a estrutura do elemento: que elementos são elementos filho de outros, a sequência pela qual os elementos filho podem aparecer e o número de elementos filho. Define igualmente se um elemento está vazio ou se pode conter texto. Este esquema pode ainda valores por defeito para alguns dos atributos. Um esquema é funcionalmente equivalente a um DTD mas é completamente escrito em XML.

Especificação DTD do sistema OpenSDRM

Nesta secção encontra-se definida a especificação DTD (*Document Type Definition*) de todas as mensagens, dados e credenciais utilizadas pela parte transaccional do OpenSDRM.

O DTD corresponde a uma descrição formal da estrutura dos documentos XML e do conteúdo que estes podem conter. Descrevem de uma forma efectiva o formato dos documentos XML, representando a estrutura e os elementos que são aceites no documento XML.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- edited with XML Spy v4.2 U (http://www.xmlspy.com) by Carlos Serrao -->
<!ELEMENT certificate (version, issuer_data, subject_data, validity, signature)>
<!ELEMENT version (#PCDATA)>
<!ELEMENT issuer_data (sig_algo_info, issuer_name, public_key)>
<!ELEMENT sig_algo_info (#PCDATA)>
<!ELEMENT issuer_name (#PCDATA)>
<!ELEMENT subject_data (subject_name?, public_key?, license?)>
<!ELEMENT subject_name (#PCDATA)>
<!ELEMENT public_key (algorithm_id, rsa_e, rsa_n, hash_of_key)>
<!ELEMENT private_key (algorithm_id, rsa_e, rsa_n, rsa_d, rsa_p, rsa_q, hash_of_key)>
<!ELEMENT algorithm_id (#PCDATA)>
<!ELEMENT rsa_e (#PCDATA)>
<!ELEMENT rsa_n (#PCDATA)>
<!ELEMENT rsa_d (#PCDATA)>
<!ELEMENT rsa_p (#PCDATA)>
<!ELEMENT rsa_q (#PCDATA)>
<!ELEMENT hash_of_key (#PCDATA)>
<!ELEMENT validity (not_before, not_after)>
<!ELEMENT not_before (#PCDATA)>
```

```
<!ELEMENT not_after (#PCDATA)>
<!ELEMENT signature (#PCDATA)>
<!ELEMENT license (content_id?, ucp_id?, ecp_id?, order_id?, contents*)>
<!ELEMENT content_id (#PCDATA)>
<!ELEMENT ucp_id (#PCDATA)>
<!ELEMENT ecp_id (#PCDATA)>
<!ELEMENT order_id (#PCDATA)>
<!ELEMENT contents (#PCDATA)>
<!ATTLIST contents
	id (usage_r_play | usage_r_copies | value) #REQUIRED
>
<!ELEMENT message (msg_contents*)>
<!ELEMENT msg_contents (#PCDATA)>
<!ATTLIST msg_contents
	id (type | content_id | order_id | ucp_id | result) #REQUIRED
>
```

Notação Textual (XSD)

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- edited with XML Spy v4.2 U (http://www.xmlspy.com) by pontocom (pontocom) -->
<!--W3C Schema generated by XML Spy v4.2 U (http://www.xmlspy.com)-->
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
	<xs:element name="algorithm_id" type="xs:string"/>
	<xs:element name="certificate">
		<xs:complexType>
			<xs:sequence>
				<xs:element ref="version"/>
				<xs:element ref="issuer_data"/>
				<xs:element ref="subject_data"/>
				<xs:element ref="validity"/>
				<xs:element ref="signature"/>
			</xs:sequence>
		</xs:complexType>
	</xs:element>
	<xs:element name="content_id" type="xs:string"/>
	<xs:element name="contents">
		<xs:complexType>
			<xs:simpleContent>
				<xs:extension base="xs:string">
					<xs:attribute name="id" use="required">
						<xs:simpleType>
							<xs:restriction base="xs:NMTOKEN">
								<xs:enumeration value="usage_r_play"/>
								<xs:enumeration value="usage_r_copies"/>
								<xs:enumeration value="value"/>
							</xs:restriction>
						</xs:simpleType>
					</xs:attribute>
				</xs:extension>
			</xs:simpleContent>
		</xs:complexType>
	</xs:element>
	<xs:element name="ecp_id" type="xs:string"/>
	<xs:element name="hash_of_key" type="xs:string"/>
	<xs:element name="issuer_data">
		<xs:complexType>
			<xs:sequence>
```

```
                        <xs:element ref="sig_algo_info"/>
                        <xs:element ref="issuer_name"/>
                        <xs:element ref="public_key"/>
                </xs:sequence>
        </xs:complexType>
</xs:element>
<xs:element name="issuer_name" type="xs:string"/>
<xs:element name="license">
        <xs:complexType>
                <xs:sequence>
                        <xs:element ref="content_id" minOccurs="0"/>
                        <xs:element ref="ucp_id" minOccurs="0"/>
                        <xs:element ref="ecp_id" minOccurs="0"/>
                        <xs:element ref="order_id" minOccurs="0"/>
                        <xs:element ref="contents" minOccurs="0" maxOccurs="unbounded"/>
                </xs:sequence>
        </xs:complexType>
</xs:element>
<xs:element name="message">
        <xs:complexType>
                <xs:sequence>
                        <xs:element ref="msg_contents" minOccurs="0" maxOccurs="unbounded"/>
                </xs:sequence>
        </xs:complexType>
</xs:element>
<xs:element name="msg_contents">
        <xs:complexType>
                <xs:simpleContent>
                        <xs:extension base="xs:string">
                                <xs:attribute name="id" use="required">
                                        <xs:simpleType>
                                                <xs:restriction base="xs:NMTOKEN">
                                                        <xs:enumeration value="type"/>
                                                        <xs:enumeration value="content_id"/>
                                                        <xs:enumeration value="order_id"/>
                                                        <xs:enumeration value="ucp_id"/>
                                                        <xs:enumeration value="result"/>
                                                </xs:restriction>
                                        </xs:simpleType>
                                </xs:attribute>
                        </xs:extension>
                </xs:simpleContent>
        </xs:complexType>
</xs:element>
<xs:element name="not_after" type="xs:string"/>
<xs:element name="not_before" type="xs:string"/>
<xs:element name="order_id" type="xs:string"/>
<xs:element name="private_key">
        <xs:complexType>
                <xs:sequence>
                        <xs:element ref="algorithm_id"/>
                        <xs:element ref="rsa_e"/>
                        <xs:element ref="rsa_n"/>
                        <xs:element ref="rsa_d"/>
                        <xs:element ref="rsa_p"/>
                        <xs:element ref="rsa_q"/>
                        <xs:element ref="hash_of_key"/>
                </xs:sequence>
        </xs:complexType>
</xs:element>
```

```
	<xs:element name="public_key">
		<xs:complexType>
			<xs:sequence>
				<xs:element ref="algorithm_id"/>
				<xs:element ref="rsa_e"/>
				<xs:element ref="rsa_n"/>
				<xs:element ref="hash_of_key"/>
			</xs:sequence>
		</xs:complexType>
	</xs:element>
	<xs:element name="rsa_d" type="xs:string"/>
	<xs:element name="rsa_e" type="xs:string"/>
	<xs:element name="rsa_n" type="xs:string"/>
	<xs:element name="rsa_p" type="xs:string"/>
	<xs:element name="rsa_q" type="xs:string"/>
	<xs:element name="sig_algo_info" type="xs:string"/>
	<xs:element name="signature" type="xs:string"/>
	<xs:element name="subject_data">
		<xs:complexType>
			<xs:sequence>
				<xs:element ref="subject_name" minOccurs="0"/>
				<xs:element ref="public_key" minOccurs="0"/>
				<xs:element ref="license" minOccurs="0"/>
			</xs:sequence>
		</xs:complexType>
	</xs:element>
	<xs:element name="subject_name" type="xs:string"/>
	<xs:element name="ucp_id" type="xs:string"/>
	<xs:element name="validity">
		<xs:complexType>
			<xs:sequence>
				<xs:element ref="not_before"/>
				<xs:element ref="not_after"/>
			</xs:sequence>
		</xs:complexType>
	</xs:element>
	<xs:element name="version" type="xs:string"/>
</xs:schema>
```

Notação Gráfica (XSD)

schema location: C:\Documents and Settings\cjcs\My Documents\Pessoal\TeseDeMestrado\certificates\ipmspro.xsd

Elements
algorithm_id
certificate
content_id
contents
ecp_id
hash_of_key
issuer_data
issuer_name
license
message
msg_contents
not_after
not_before
order_id
private_key
public_key
rsa_d

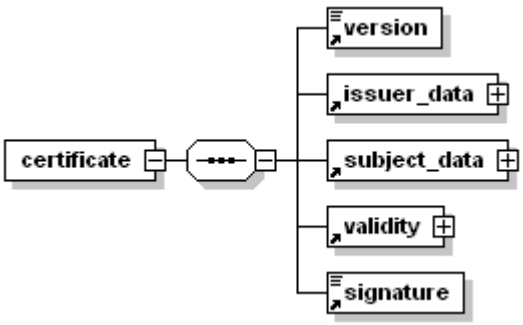
rsa_e
rsa_n
rsa_p
rsa_q
sig_algo_info
signature
subject_data
subject_name
ucp_id
validity
version

element **algorithm_id**

diagram 

type **xs:string**
used by elements private_key public_key
source
```
<xs:element name="algorithm_id" type="xs:string"/>
```

element **certificate**

diagram 

children version issuer_data subject_data validity signature
source
```
<xs:element name="certificate">
 <xs:complexType>
  <xs:sequence>
   <xs:element ref="version"/>
   <xs:element ref="issuer_data"/>
   <xs:element ref="subject_data"/>
   <xs:element ref="validity"/>
   <xs:element ref="signature"/>
  </xs:sequence>
 </xs:complexType>
</xs:element>
```

element **content_id**

diagram 

type **xs:string**
used by element license
source
```
<xs:element name="content_id" type="xs:string"/>
```

element **contents**

diagram 

type extension of **xs:string**
used by element license
attributes

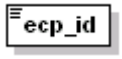
Name	Type	Use	Default	Fixed	Annotation
id	xs:NMTOKEN	required			

source
```
<xs:element name="contents">
 <xs:complexType>
  <xs:simpleContent>
   <xs:extension base="xs:string">
    <xs:attribute name="id" use="required">
     <xs:simpleType>
      <xs:restriction base="xs:NMTOKEN">
       <xs:enumeration value="usage_r_play"/>
```

```
            <xs:enumeration value="usage_r_copies"/>
            <xs:enumeration value="value"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
    </xs:extension>
  </xs:simpleContent>
 </xs:complexType>
</xs:element>
```

element **ecp_id**

diagram

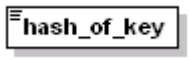


type **xs:string**
used by element **license**
source

```
<xs:element name="ecp_id" type="xs:string"/>
```

element **hash_of_key**

diagram

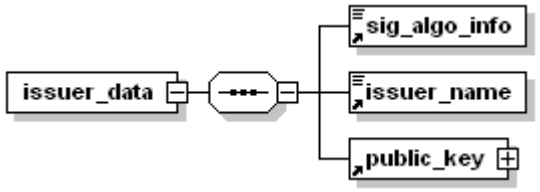


type **xs:string**
used by elements **private_key** **public_key**
source

```
<xs:element name="hash_of_key" type="xs:string"/>
```

element **issuer_data**

diagram



children **sig_algo_info** **issuer_name** **public_key**
used by element **certificate**
source

```
<xs:element name="issuer_data">
 <xs:complexType>
  <xs:sequence>
   <xs:element ref="sig_algo_info"/>
   <xs:element ref="issuer_name"/>
   <xs:element ref="public_key"/>
  </xs:sequence>
 </xs:complexType>
</xs:element>
```

element **issuer_name**

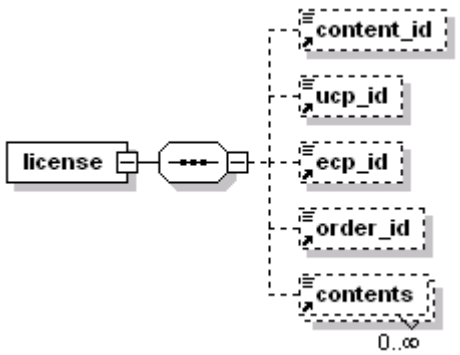
diagram

type **xs:string**
used by element **issuer_data**
source

```
<xs:element name="issuer_name" type="xs:string"/>
```

element **license**

diagram

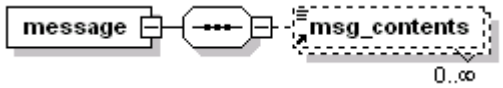


children **content_id** **ucp_id** **ecp_id** **order_id** **contents**
used by element **subject_data**

```
<xs:element name="license">
 <xs:complexType>
  <xs:sequence>
   <xs:element ref="content_id" minOccurs="0"/>
   <xs:element ref="ucp_id" minOccurs="0"/>
   <xs:element ref="ecp_id" minOccurs="0"/>
   <xs:element ref="order_id" minOccurs="0"/>
   <xs:element ref="contents" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
 </xs:complexType>
</xs:element>
```

element **message**

diagram



children **msg_contents**

```
<xs:element name="message">
 <xs:complexType>
  <xs:sequence>
   <xs:element ref="msg_contents" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
 </xs:complexType>
</xs:element>
```

element **msg_contents**

diagram

type extension of **xs:string**
used by element **message**

attributes	Name	Type	Use	Default	Fixed	Annotation
	id	xs:NMTOKEN	required			

```
<xs:element name="msg_contents">
 <xs:complexType>
  <xs:simpleContent>
   <xs:extension base="xs:string">
    <xs:attribute name="id" use="required">
     <xs:simpleType>
      <xs:restriction base="xs:NMTOKEN">
       <xs:enumeration value="type"/>
       <xs:enumeration value="content_id"/>
       <xs:enumeration value="order_id"/>
       <xs:enumeration value="ucp_id"/>
       <xs:enumeration value="result"/>
      </xs:restriction>
     </xs:simpleType>
    </xs:attribute>
   </xs:extension>
  </xs:simpleContent>
 </xs:complexType>
</xs:element>
```

element **not_after**

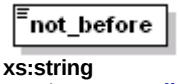
diagram

type **xs:string**
used by element **validity**

```
<xs:element name="not_after" type="xs:string"/>
```

element **not_before**

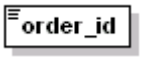
diagram



type **xs:string**
used by element **validity**

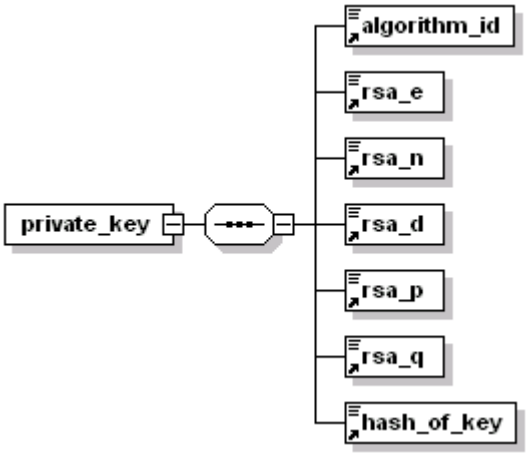
```
<xs:element name="not_before" type="xs:string"/>
```

element **order_id**

diagram 

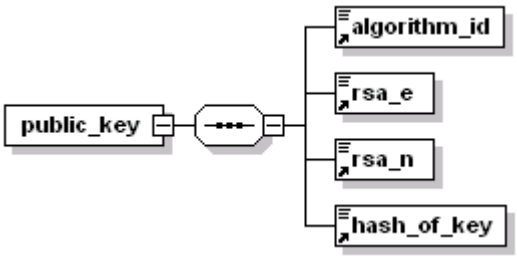
type **xs:string**
used by element **license**
source
```
<xs:element name="order_id" type="xs:string"/>
```

element **private_key**

diagram 

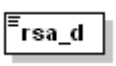
children **algorithm_id rsa_e rsa_n rsa_d rsa_p rsa_q hash_of_key**
source
```
<xs:element name="private_key">
 <xs:complexType>
  <xs:sequence>
   <xs:element ref="algorithm_id"/>
   <xs:element ref="rsa_e"/>
   <xs:element ref="rsa_n"/>
   <xs:element ref="rsa_d"/>
   <xs:element ref="rsa_p"/>
   <xs:element ref="rsa_q"/>
   <xs:element ref="hash_of_key"/>
  </xs:sequence>
 </xs:complexType>
</xs:element>
```

element **public_key**

diagram 

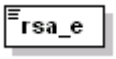
children **algorithm_id rsa_e rsa_n hash_of_key**
used by elements **issuer_data subject_data**
source
```
<xs:element name="public_key">
 <xs:complexType>
  <xs:sequence>
   <xs:element ref="algorithm_id"/>
   <xs:element ref="rsa_e"/>
   <xs:element ref="rsa_n"/>
   <xs:element ref="hash_of_key"/>
  </xs:sequence>
 </xs:complexType>
</xs:element>
```

element **rsa_d**

diagram 

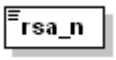
type **xs:string**
used by element **private_key**
source
```
<xs:element name="rsa_d" type="xs:string"/>
```

element **rsa_e**
diagram



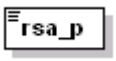
type **xs:string**
used by elements **private_key** **public_key**
source
```
<xs:element name="rsa_e" type="xs:string"/>
```

element **rsa_n**
diagram



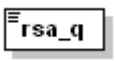
type **xs:string**
used by elements **private_key** **public_key**
source
```
<xs:element name="rsa_n" type="xs:string"/>
```

element **rsa_p**
diagram



type **xs:string**
used by element **private_key**
source
```
<xs:element name="rsa_p" type="xs:string"/>
```

element **rsa_q**
diagram



type **xs:string**
used by element **private_key**
source
```
<xs:element name="rsa_q" type="xs:string"/>
```

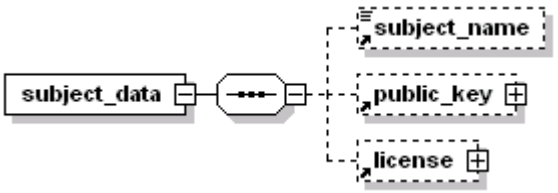
element **sig_algo_info**
diagram

type **xs:string**
used by element **issuer_data**
source
```
<xs:element name="sig_algo_info" type="xs:string"/>
```

element **signature**
diagram

type **xs:string**
used by element **certificate**
source
```
<xs:element name="signature" type="xs:string"/>
```

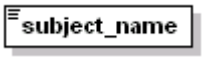
element **subject_data**
diagram



children **subject_name** **public_key** **license**
used by element **certificate**
source
```
<xs:element name="subject_data">
 <xs:complexType>
  <xs:sequence>
   <xs:element ref="subject_name" minOccurs="0"/>
   <xs:element ref="public_key" minOccurs="0"/>
   <xs:element ref="license" minOccurs="0"/>
```

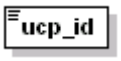
```
    </xs:sequence>
  </xs:complexType>
</xs:element>
```

element **subject_name**

diagram 

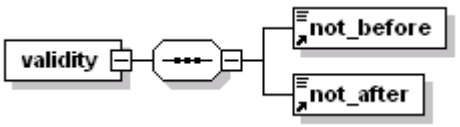
type **xs:string**
used by element **subject_data**
source
```
<xs:element name="subject_name" type="xs:string"/>
```

element **ucp_id**

diagram 

type **xs:string**
used by element **license**
source
```
<xs:element name="ucp_id" type="xs:string"/>
```

element **validity**

diagram 

children **not_before** **not_after**
used by element **certificate**
source
```
<xs:element name="validity">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="not_before"/>
      <xs:element ref="not_after"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
```

element **version**

diagram 

type **xs:string**
used by element **certificate**
source
```
<xs:element name="version" type="xs:string"/>
```

ANEXO E – QUESTIONÁRIO DE UTILIZAÇÃO DO SISTEMA

Fase 1: Implementação

A ser preenchido por todos os participantes.

1. Indique idade e sexo.				
Idade:	…….. anos		Sexo:	M / F
2. Indique o seu nível de utilização em informática.				
Em casa:	nunca	< 1 hora por dia	1-3 horas por dia	>3 horas por dia
No serviço/trabalho:	nunca	ocasionalmente	Várias vezes ao dia	continuamente
3. Como descreve as suas competências em informática?				
Iniciado		Intermédio		Perito
4. Qual o seu nível de utilização da Internet?				
Em casa:	nunca	< 1 hora por dia	1-3 horas por dia	>3 horas por dia
No serviço/trabalho:	nunca	Ocasionalmente	Várias vezes ao dia	Continuamente
5. . Como descreve as suas competências na utilização da Internet?				
Iniciado		Intermédio		Perito
6. Quais os seus objectivos ao tomar parte nestes Testes?				
Texto livre…				
7. O que espera deste Testes?				

Texto livre...

Fase 2: Instalação

Para ser preenchido pelos participantes que possuem o sistema OCCAMM instalado nas suas máquinas.

1. Instalou o sistema OCCAMM em casa ou no Serviço/Local de trabalho?
Casa Serviço
2. Classifique a instalação de cada componente do sistema numa escala de 1 a 5 (1=muito simples, 5=muito difícil). Se não instalou um dos componentes anote com "n/a".
Instalação e configuração do software Acompanhamento das instruções de instalação
3. Quanto tempo demorou a instalação na sua totalidade?
<1 HORA 1-2 HORAS 2-3 HORAS >3 HORAS
4. Descreva possíveis problemas que tenha encontrado.
Texto livre…
5. Foram esses problemas correctamente? Como?
Texto livre…

Fase 3: 1°Mês

A ser preenchido por todos os participantes.

1. Classifique a performance dos seguintes aspectos do sistema numa escala de 1 a 5 (1=muito fraca, 5=muito boa). Se não instalou um dos componentes anote com "n/a".
Site de Web

(ie.O *site* de web era claro e simples de utilizar). *eCommerce* (ie. O pagamento do material era fácil ou difícil) *Download* do material multimedia (ie. Quanto tempo demorou até obter os ficheiros pretendidos) Visualizar/ouvir o material multimedia (ie. Quanto tempo demorou a operação relativa aos procedimentos de segurança e a ganhar acesso ao material multimedia).
2. Qual a sua percepção do valor do sistema, numa escala de 1 a 5
3. Por favor comente os pontos a favor e os contra do sistema.
Texto livre…
4. Qual a sua percepção da utilidade deste sistema, numa escala (1= muito baixa, 5=muito alta).
5. Por favor comente os pontos a favor e os contra.
Texto livre…

Fase 4 : 2° mês

A ser preenchido pelos participantes dos testes em que estão a ser conduzidas serviços/experiências adicionais no decorrer do Segundo mês.

1. Como classifica a performance de cada uma das funcionalidades utilizadas no decorrer do Segundo mês, numa escala de 1 a 5 (1=Muito fraca, 5=Muito boa). Se não utilizou um dos componentes/aspecto anote com "n/a"
Dois sistemas de controlo de acessos alternativos. Sistema Smartcard. *Wallet* (descreva).

2. Comente os pontos bons e maus.
Texto livre…
3. Quais as melhorias ou funcionalidades acrescidas que gostaria de ver implementadas?
Texto livre…

Fase 5: Finalização

A ser preenchido por todos os participantes.

1. Como classifica a praticabilidade do sistema, numa escala de 1 a 5 (1= muito fraca, 5= muito boa)?
2. Qual o seu nível de satisfação com o sistema, tendo em conta os seus objectivos e expectativas iniciais, numa escala de 1 a 5 (1= muito baixa, 5= muito alta)?
3. Identifique os pontos fortes e fracos do sistema (qual a sua opinião).
Texto livre…
4. Qual o seu interesse em futuramente usar um serviço destes no seu trabalho/laser, numa escala de 1 a 5 (1= muito pouco, 5= muitíssimo)?
5. Pode sugerir algumas melhorias?
Texto livre…

ANEXO F – CRIPTOGRAFIA, CERTIFICADOS E PKI

Algoritmo	Tamanho da chave	Ciclos	Aplicação
DES	56 bits	16	SET, *Kerberos*
Triple DES	112 ou 168 bits	48	PGP, S/MIME
IDEA	128 bits	8	PGP
Blowfish	Variável até 448 bits	16	
RC5	Variável até 2048 bits	Variável até 255	
CAST-128	40 até 128 bits	16	

Tabela F.1 – Algoritmos de criptografia convencional

Algoritmo	Encriptação/ Desencriptação	Assinatura Digital	Troca de Chaves
RSA	Sim	Sim	Sim
Diffie-Hellman	Não	Não	Sim
DSS	Não	Sim	Não
Curva Elíptica	Sim	Sim	Sim

Tabela F.2 – Aplicação de Sistemas de criptografia de chave pública

Troca de Chaves Diffie-Hellman	
Elementos Globais e Públicos	
Q	número primo
α	α<q e α é uma raiz primitiva de q
O utilizador A gera o seguinte	
Selecciona X_A privado	X_A<q
Calcula Y_A público	$Y_A = a^{X_A} \bmod q$
O utilizador B gera o seguinte	
Selecciona X_B privado	X_B<q
Calcula Y_B público	$Y_B = b^{X_B} \bmod q$
Geração da chave secreta pelo utilizador A	
$K = (Y_B)^{X_A} \bmod q$	
Geração da chave secreta pelo utilizador B	
$K = (Y_A)^{X_B} \bmod q$	

Tabela F.3 Troca de chaves Diffie-Hellman

Algoritmo RSA
Geração de chaves
Seleccionar ‘p’ e ‘q’ em que ambos são primos Calcular n=pxq Calcular $f(n) = (p-1)(q-1)$ Seleccionar ‘e’ tal que $mdc(f(n), e) = 1;\ 1 < e < f(n)$ Calcular ‘d’ tal que $d = e^{-1} \bmod f(n)$ Chave Pública: KU={e,n} Chave Privada: KR={d,n}
Encriptação
Texto simples: M<n Texto encriptado: $C = M^e \pmod n$
Desencriptação
Texto encriptado: C Texto simples: $M = C^d \pmod n$

Tabela F.4 Descrição do funcionamento do RSA

Assinaturas Digitais Cegas
Assuma-se que um determinado receptor deseja obter uma assinatura digital numa mensagem *m*, em que *m* corresponde a um número inteiro entre 0 e *n*. O protocolo consiste nas seguintes fases:
Blinding
O receptor escolhe um factor de *blinding r*, que é um número aleatório entre 0 e *n*, e calcula o valor $m' = mr^e \bmod n$. O receptor envia *m’* para o assinante
Assinatura
O assinante usa a sua chave privada *d* para calcular o valor $s' = m'^d \bmod n$, retornando o valor *s’* para o receptor
Unblinding
Receptor extrai a assinatura $s = s'/r \bmod n$
O receptor fica então com o par (*m*, *s*) que satisfaz a equação $s = me \bmod n$ que é a forma como se processa a verificação de assinaturas do RSA. O assinante não sabe que mensagem *m* assinou devido ao factor aleatório *r*.

Tabela F.5 Algoritmo de Assinaturas Digitais Cegas

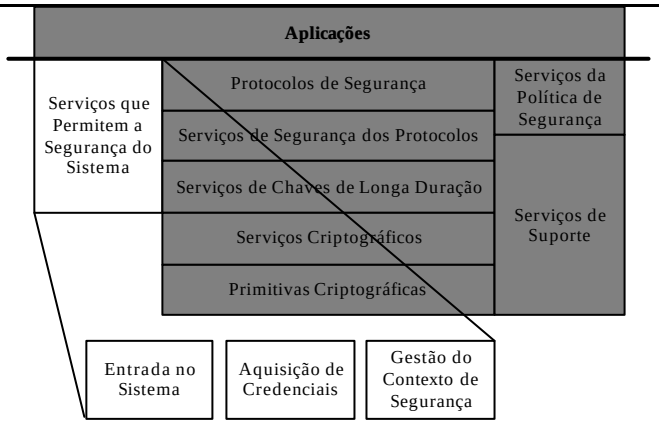
Normas de Criptografia de Chave Pública	
O PKCS ou *Public Key Criptographic Standards* foram desenvolvidos pelos laboratórios da RSA em colaboração com outros parceiros para melhorar a interoperabilidade dos produtos de criptografia de chave pública. As normas PKCS oferecem as definições fundamentais dos formatos de dados e de algoritmos que suportem a maior parte das implementações de PKI existentes	
PKCS#1	Norma de encriptação RSA
PKCS#2	(incorporado no PKCS#1)
PKCS#3	Norma de troca de chaves Diffie-Hellman
PKCS#4	(incorporado no PKCS#1)
PKCS#5	Norma de encriptação baseada em palavra-chave
PKCS#6	Norma de sintaxe de extensões de certificados
PKCS#7	Norma de sintaxe de mensagem criptográfica
PKCS#8	Norma de sintaxe de informação da chave privada
PKCS#9	Tipos de atributos seleccionados
PKCS#10	Normas de sintaxe do pedido de certificação
PKCS#11	Norma de interface de senhas criptográficas
PKCS#12	Norma de sintaxe de troca de informação pessoal
PKCS#13	Norma de criptografia de curva elíptica
PKCS#14	Norma de geração de números pseudo aleatórios
PKCS#15	Norma de sintaxe de informação de senha criptográfica

Tabela F.6 Normas de Criptografia de Chave Pública

Tipo	Descrição	Observações
CRLs	Estrutura de dados assinados que contém uma lista de certificados revogados (X.509)	Criticado do ponto de vista da performance, escalabilidade e oportunidade. Existem no entanto algumas alternativas que permitem melhorar o aspecto da performance e da escalabilidade
ARLs	Um tipo de CRL dedicado exclusivamente a informação de revogação de CAs (X.509)	A separação entre o utilizador final e a CA é lógica e encontra-se em diversas implementações
DpCRLs	Um método normalizado de repartição de informação de CRL (X.509)	Oferece algumas melhorias em termos de performance e de escalabilidade no entanto a

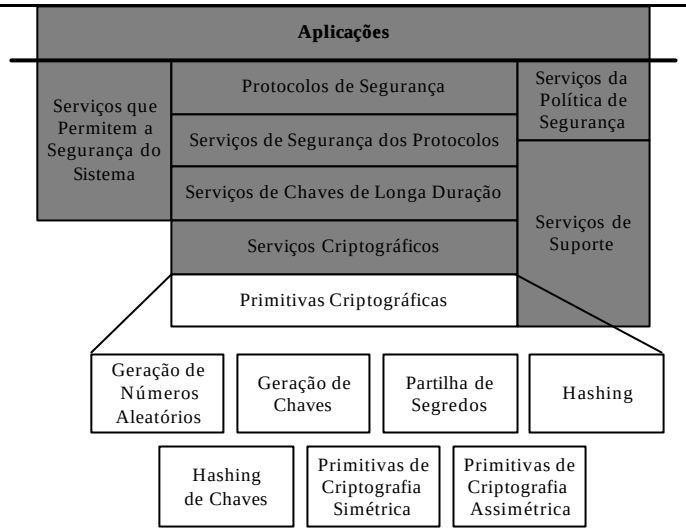
		questão de oportunidade permanece
dCRLs	Um método normalizado para enviar informação de revogação temporariamente sem necessitar de uma CRL completa ou de uma actualização DpCRLs (X.509)	Pode ser usado em conjunto com a DpCRL para obter melhorias a nível da performance, escalabilidade e oportunidade
iCRLs	Um método normalizado que permite que a informação de revogação de várias CAs pode coexistir no mesmo CRL (X.509)	Pode ser usado para melhorar a performance
DEpCRLs	Conceito recente para suportar partilha dinâmica de CRLs tal como vários métodos de questionar informação de revogação (X.509)	
CRTs	Tecnologia que permite que a informação de revogação possa ser expressa em árvores binárias (ValidCert)	
OCSP	Um protocolo para verificar *on-line* o estado de um ou de vários certificados (RFC2560)	Apesar de oferecer um método *on-line*, está dependente da capacidade de resposta do próprio serviço de revogação.

Tabela F.7 Tabela comparativa dos Mecanismos de Revogação de Certificados

Modelo APKI	
Serviços que Permitem a Segurança do Sistema	
Certas funções do sistema são absolutamente necessárias para suportar serviços de Entrada no Sistema, Obtenção de Credenciais e de Gestão do Contexto de Segurança (através da associação da informação de segurança com os processos de um determinado utilizador).	
Primitivas Criptográficas	

Estes componentes proporcionam o acesso a primitivas criptográficas de baixo nível, tais como geração de chaves, funções de *hash*, encriptação e desencriptação utilizando algoritmos de chave secreta e de chave pública, entre outros.

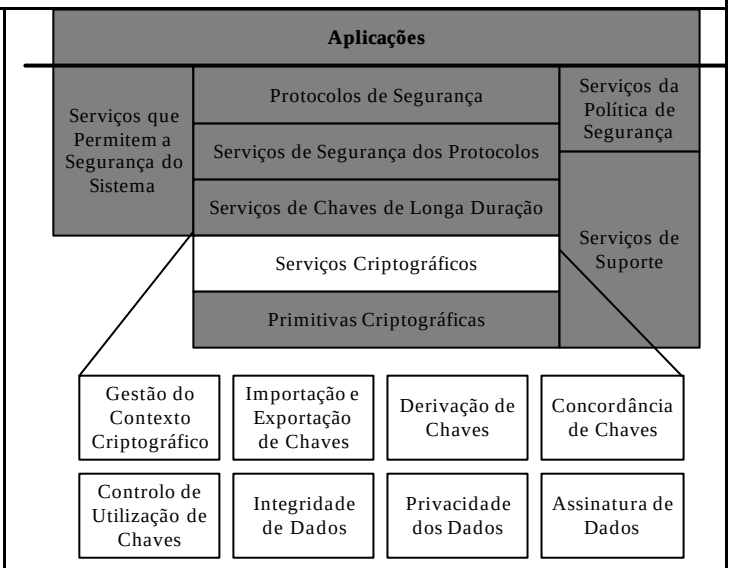
Estas Primitivas Criptográficas são normalmente invocadas localmente e não necessitam de qualquer protocolo de comunicação entre si.



Serviços Criptográficos

Este tipo de componentes proporciona o acesso a serviços criptográficos diversos tais como integridade de dados e protecção de confidencialidade, importação e exportação de chaves, assinaturas digitais entre outros.

A Gestão do Contexto Criptográfico proporciona funcionalidades através das quais as aplicações inicializam os subsistema criptográfico, activam as chaves para encriptação e desencriptação e terminam o subsistema criptográfico após este deixar de ser necessário.



O Controlo de Utilização de Chaves permite o controlo de uma variedade de aspectos da utilização de chaves, incluindo o número de vezes que uma determinada chave pode ser utilizada, para que tipo de utilização entre outros.

Os Serviços de Derivação de Chaves permitem a geração de chaves com qualidade criptográfica através de valores não-chave, tais como palavras-chave.

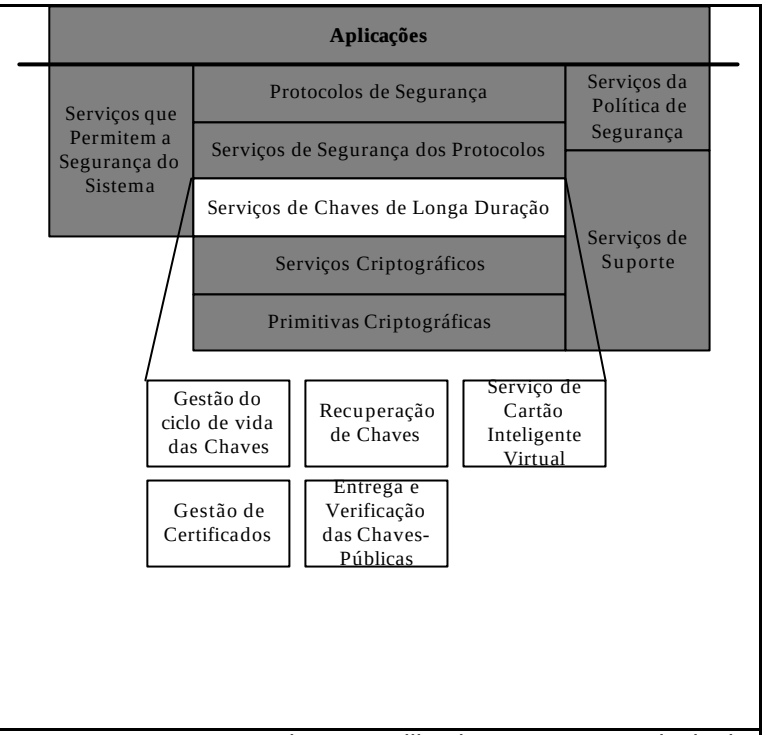
Os Serviços Criptográficos estão construídos sobre as Primitivas Criptográficas. Um Serviço criptográfico pode suportar múltiplas implementações, cada uma delas utilizando diferentes primitivas criptográficas. Estes Serviços Criptográficos são normalmente invocados localmente e não necessitam de qualquer protocolo de comunicação entre si.

Serviços de Chaves de Longa Duração

As diversas funções deste componente são as seguintes:

Gestão do ciclo das Chaves: entre as funções que este componente disponibiliza incluem-se a geração de chaves, requisição de certificados, revogação de chaves, repúdio de chaves, a expiração de chaves e outros serviços associados;

Recuperação de Chaves: esta componente suporta a preparação de chaves para recuperação, e permite a sua recuperação posterior sob o controlo de uma determinada política;



Serviço de Cartão Inteligente Virtual: esta componente permite que utilizadores e outros principais possam armazenar informação pessoal de segurança a longo prazo (que pode incluir chaves privadas, certificados ou outro tipo de informação) em meios de armazenamento protegido, para activação de chaves pessoais para utilização através de processos de autenticação e para utilizar essas mesmas chaves para actividades de encriptação, desencriptação ou assinatura;

Gestão de Certificados: esta componente permite que utilizadores, administradores e outros principais possam solicitar certificados de chave pública e revogar certificados previamente requeridos. Pode ainda opcionalmente gerar chaves e fornecer serviços de recuperação de chaves. Este componente é composto por quatro sub-componentes: Autoridade Local de Registo, Agente da Autoridade de Certificação, Autoridade de Certificação e Autoridade de Publicação.

A Autoridade Local de Registo proporciona interfaces para o pedido de pares de chaves e os correspondentes certificados, pedidos da certificação de chaves públicas existentes e pedidos de revogação de certificados;

O Agente da Autoridade de Certificação fornece interfaces para a certificação de chaves públicas existentes, gerando e retornando pares de chaves e os correspondentes certificados, e revogando os certificados. Este Agente da Autoridade de Certificação implementa estas interfaces através da utilização dos serviços da Autoridade de Certificação;

A Autoridade de Certificação certifica chaves públicas, retornando os correspondentes certificados e gera as Listas de Revogação de Certificados (CRLs). Em alguns casos este processo pode ocorrer off-line;

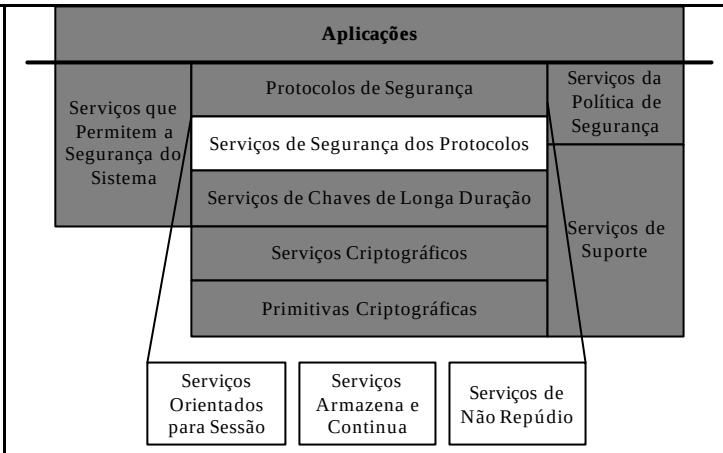
A Autoridade de Publicação fornece interfaces através dos quais a Autoridade de Certificação e os Agentes da Autoridade de Certificação podem colocar certificados e CRLs em repositórios públicos ou transmiti-los directamente para os requisitantes.

Entrega e Verificação de Chaves Públicas: esta componente permite que um programa recupere

um certificado de um qualquer principal, verificar a sua validade e extrair a chave pública certificada do certificado do principal.;

Serviços de Segurança dos Protocolos

Os Serviços de Segurança dos Protocolos estão divididos em dois tipos fundamentais: Orientados por Sessão e Armazena e Continua.



Orientados por Sessão: serviços de segurança que requerem entidades de exploração para manter informação acerca do estado de segurança associado com as trocas de protocolo.

Armazena e Continua: serviços de segurança que encapsulam toda a informação acerca do estado de segurança dentro das senhas protegidas que geram. Estes serviços ao contrário dos anteriores não requerem a utilização de entidades de exploração para manter a informação acerca do estado de segurança.

Estes componentes proporcionam serviços de segurança apropriados para quem concebe pilhas de protocolos. Estas componentes proporcionam as seguintes funções:

Proporcionam um mecanismo de segurança e protocolos de negociação da qualidade de protecção utilizáveis por parceiros que queiram comunicar entre si e que necessitam de concordar num determinado regime de segurança;

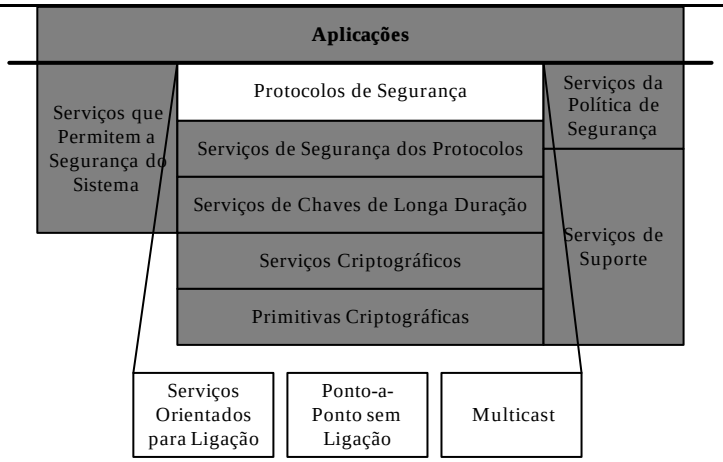
Gerem a informação do estado de segurança necessário pelos parceiros do protocolo que desejem construir e manter associações seguras entre si;

Encapsulamento da autenticação da origem dos dados, protecção de dados, transporte transparente de credenciais e privilégios num único serviço;

Aplicação de mecanismos de segurança baseados em informação da política a ser administrada.

Protocolos de Segurança

Existem diversos tipos de protocolos seguros, que se podem englobar genericamente em três categorias distintas: Orientados por Ligação Ponto a Ponto, Sem Ligação Ponto a Ponto, e *Multicast*.



Orientados por Ligação Ponto a Ponto: estes protocolos permitem que exactamente dois parceiros, em que cada um deles deve estar *on-line*,

comuniquem em segurança;

Sem Ligação Ponto a Ponto: estes protocolos permitem que exactamente dois parceiros, em que um ou ambos podem estar off-line em algum intervalo de tempo durante o qual mensagens são transmitidas, comuniquem em segurança;

Multicast: estes protocolos permitem que uma entidade comunique em segurança e simultaneamente com vários parceiros. Algumas dessas entidades podem estar off-line durante um determinado período de tempo, durante o qual mensagens são transmitidas.

Os protocolos seguros proporcionam a transferência segura de dados entre parceiros de comunicação sem necessitar de quaisquer chamadas aos serviços de segurança. As aplicações que utilizem protocolos de segurança podem ter que especificar a qualidade desejada de protecção antes de iniciar o estabelecimento do protocolo

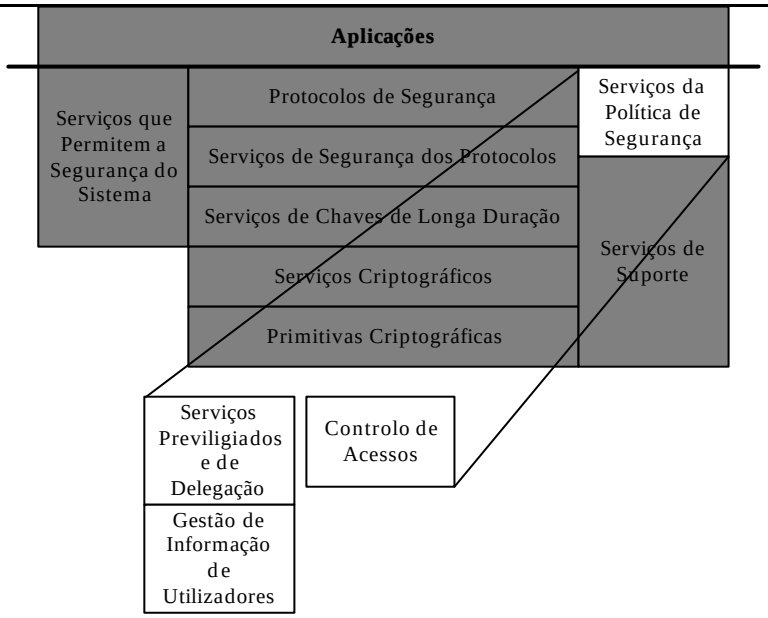
Serviços da Política de Segurança

Estes serviços gerem a informação acerca dos privilégios dos utilizadores e as políticas de controlo de acessos a recursos, e tomam decisões relativamente ao controlo de acessos baseando-se nessa informação. As componentes destes serviços são:

Serviços de Delegação de Privilégios;

Gestão de Informação dos Utilizadores;

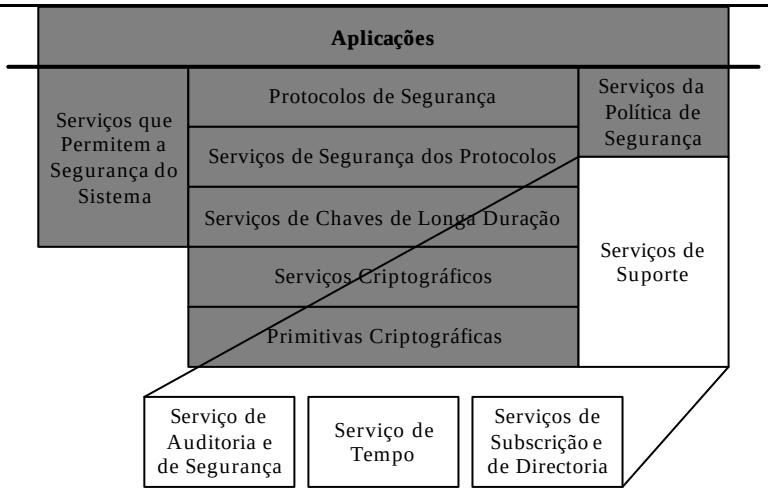
Controlo de Acessos.



Serviços de Suporte

Estas componentes proporcionam funções requisitadas pelos serviços de segurança ou requisitada pela operação segura de um sistema de rede, não impondo, no entanto, nenhuma política de segurança.

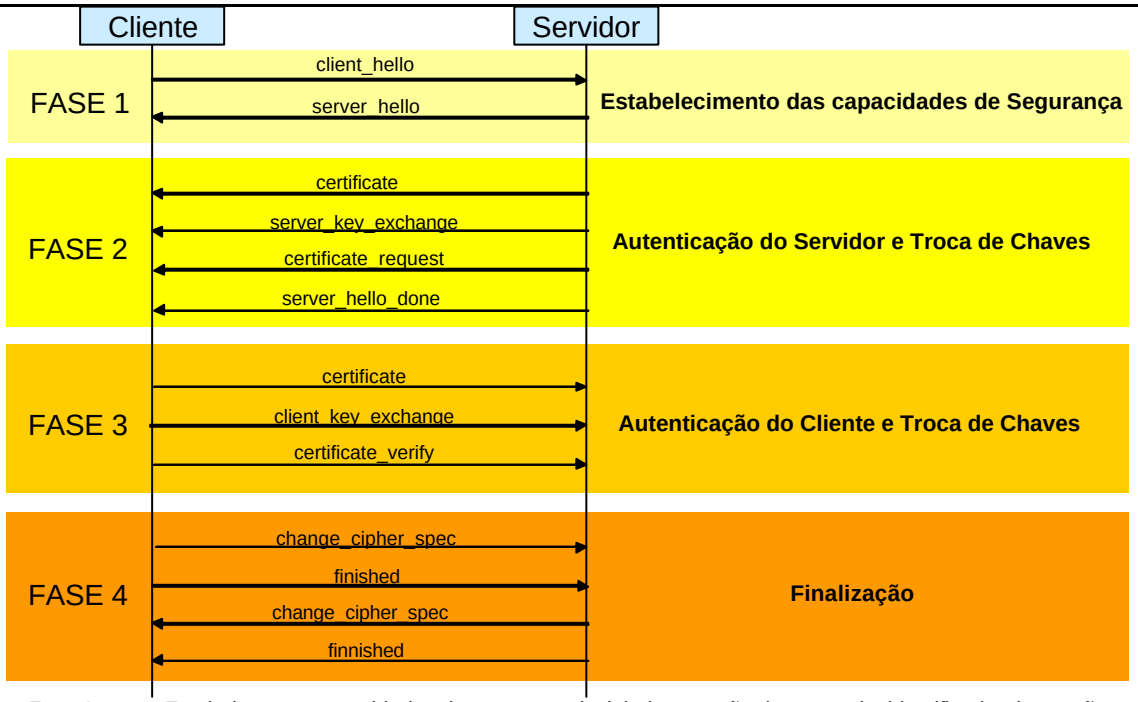
Serviço de Auditoria e Segurança: suporta todas as funções de registo de ocorrências e dentro da arquitectura de PKI e pode igualmente suportar serviços



de notariado; **Serviço de Tempo**: este serviço é fundamental para a sincronização de tempo dentro de uma arquitectura PKI distribuída, sendo ainda a base para os *timestamps* que podem ser incorporados nos certificados de segurança e que são igualmente utilizados pelos serviços de notário; **Serviços de Subscrição e de Directoria**: estes serviços são absolutamente necessários para permitir a localização de utilizadores da arquitectura PKI assim como a consulta de todos os atributos aplicáveis aos mesmos.	

Tabela F.8 Descrição do modelo APKI

Protocolo *Handshake*
O protocolo *Handshake* é composto por três sub-protocolos (*Handshake*, *Alert*, *ChangeCipherSpec*) que permitem que as aplicações em comunicação possam acordar sobre os parâmetros de segurança para o protocolo *Record*, que se autentiquem, instanciem os parâmetros de segurança e de reporte de erros.



Fase 1	Estabelecer as capacidades de segurança, incluindo a versão do protocolo, identificador de sessão, conjunto de algoritmos, método de compressão e números aleatórios
Fase 2	O servidor pode enviar certificados, trocar as chaves e pedir o certificado ao cliente. O servidor assinala o fim da fase da mensagem de 'hello'
Fase 3	Cliente envia certificado se pedido. Cliente envia chave. Cliente pode enviar verificação do certificado
Fase 4	Troca de algoritmos termina e termina o protocolo *Handshake*

Tabela F.9 Protocolo Handshake do SSL/TLS

Protocolo *Record*

Este protocolo é composto por diversas sub-camadas. Processa os dados das aplicações através da fragmentação dos mesmos em blocos de menor dimensão, comprimindo-os (opcionalmente) e calculando os valores correspondentes de integridade, encriptando os dados das camadas superiores e transmitindo-os. Serve essencialmente para encapsular todas as mensagens do SSL/TLS, oferecendo este serviço a todas as mensagens dos restantes protocolos de nível superior (*Handshake*, *Alert*, *ChangeCipherSpec* e outros dependentes da aplicação).

	Protocolo	Versão	Tamanho	Mensagem	MAC	

Tabela F.10 Protocolo Record do SSL/TLS

ANEXO G – ANÁLISE DO SECTOR DA MÚSICA

Análise do sector de Música

O sector da Música está estabilizado e tem funcionado quase sempre sem sofrer alterações profundas ao longo do tempo. Entre as alterações que se verificaram neste sector destacam-se o aparecimento de formatos diversos de suporte físico de música (cassete, disco (Single, LP)), no entanto, a alteração mais profunda apenas aconteceu com a introdução do formato Compact-Disc. Este último acontecimento, aliado ao crescente aparecimento de leitores de CD-Rom nos computadores pessoais, fizeram com que fosse fácil para qualquer um extrair as faixas musicais dos CDs e armazená-las noutro suporte que não o CD [OCBMS00].

Igualmente, o crescimento da Internet, aliado ao desenvolvimento de formas de codificação e compressão mais eficientes das faixas musicais veio facilitar a troca das mesmas entre milhões de utilizadores [OCOLSMD00].

Os dois factores anteriormente referidos marcam uma das mudanças que o sector da música tem que enfrentar e representam igualmente um dos maiores desafios desta poderosa indústria. Como resposta, surgiram vários modelos para distribuição de música digital.

A Cadeia de Valor

Apesar do papel crucial que desempenha na criação de conteúdo, o poder do artista na cadeia de valor depende em grande parte do seu nível de popularidade. Quanto mais popular for o artista mais poderoso é o seu papel na cadeia de valor, e apesar do seu sucesso depender de factores pessoais tais como as suas capacidades vocais ou da letra da música, o mais provável é que o esforço promocional da imagem do artista por parte da editora discográfica seja a condicionante principal do seu sucesso. A imagem em conjunto com o tipo de música decide a procura pela música do mesmo e igualmente a quantidade de receitas geradas. Por sua vez, isto determina o seu status na cadeia de valor, assim como o valor dos direitos de autor que o artista pode reclamar junto da editora discográfica [OCBMS00].

O papel da editora discográfica é principalmente o de monitorização e promoção da música através de discos e de aparições em público dos artistas. Desempenha um determinado número de funções na cadeia de valor, tais como: contratação de artistas, selecção e revisão de música, gravação, promoção e distribuição de álbuns, entre outras. Devido ao número de funções que desempenha, a editora discográfica é o actor mais forte na cadeia de valor, controlando ainda, muitas vezes, igualmente, o processo criativo e de comercialização [OCBMS00].

No entanto, e uma vez que num sistema de distribuição essencialmente físico é impossível para uma editora discográfica deter relações individuais de distribuição com cada consumidor, a editora depende ainda da distribuição de lojas locais para levar a música até ao consumidor final. Como resultado, cerca de 80% das vendas de música registam-se ainda em lojas da especialidade, conferindo-lhes uma influência bastante importante na cadeia de valor [OCOLSMD00].

De seguida são apresentados dois modelos da cadeia de valor: um simplificado (Figura G.1) e outro mais completo (Figura G.2).

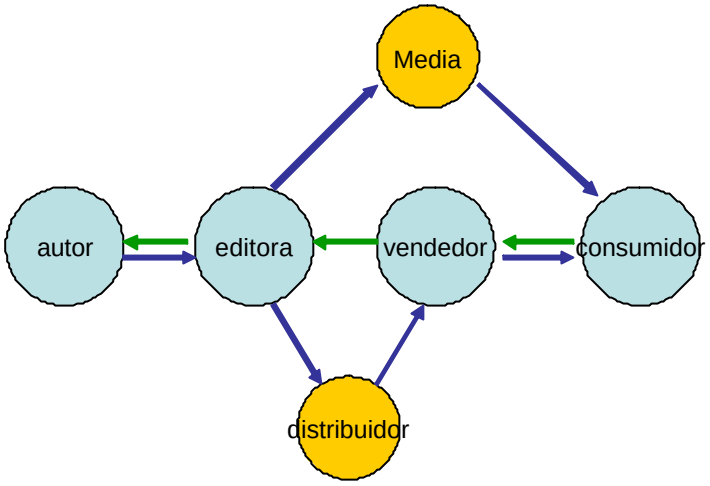


Figura G.1 Modelo simplificado da Cadeia de Valor do sector da Música

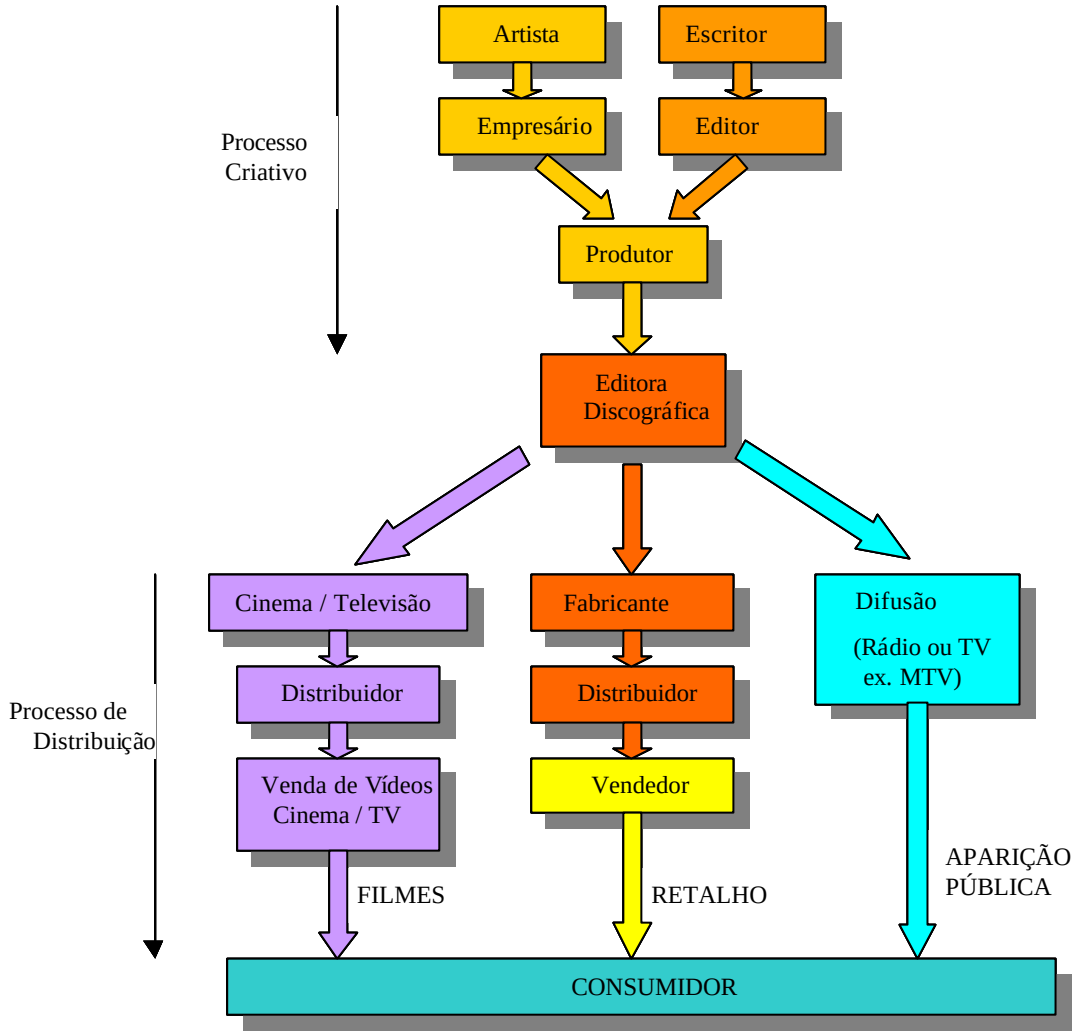


Figura G.2 Modelo completo da Cadeia de Valor do sector da Música

Actores

Os actores principais da cadeia de valor do sector da Música são: o **artista**/**autor** (o criador da música), a **editora discográfica** (aquela que publica a música) e o **vendedor**. Em conjunto, estes actores desempenham cinco funções principais da cadeia de valor do sector da música [OCECPS00, OCOLSMD00]:

- Criação (artista);
- Produção (editora discográfica);
- Distribuição (editora discográfica);
- Promoção (editora discográfica/ vendedor);
- Comercialização (vendedor).

Papéis dos vários actores

Os actores podem ser caracterizados pelos papéis que desempenham na cadeia de valor, que são os seguintes [OCOLSMD00]:

- **Criação**: criação do conteúdo digital (música) que corresponde ao valor nuclear na cadeia de valor;
- **Produção**: o conteúdo criado tem que ser ajustado e formatado num formato que seja adequado para as necessidades do mercado alvo;
- **Organização**: pode ser dividida em duas partes. A primeira parte diz respeito à organização que ocorre no início da cadeia de valor, quando o artista ou o produtor seleccionam uma série de músicas (faixas) para serem colocadas no álbum. O vendedor, desempenha a segunda parte, organizando o seu *stock* de música por géneros musicais e artistas, por exemplo, fazendo com que o consumidor possa encontrar melhor aquilo que procura no seu vasto *stock*.
- **Promoção**: este papel é desempenhado por vários actores utilizando diversos meios.
- **Distribuição**: pode ser igualmente dividido em várias partes. Em primeiro lugar, existe a distribuição entre os vários intermediários na cadeia de valor (chamada de cadeia de distribuição, que inclui actividades como armazenamento, transporte e expedição). Em segundo lugar, existe a distribuição final para o consumidor.

O quadro (Tabela G.1) seguinte sintetiza os papéis desempenhados pelos vários actores.

Actores	***Papéis***	***Valor Acrescentado***
Artista	Criador de Conteúdo	Expressão musical criativa
Editora discográfica	Produtor, Promotor, Distribuidor, Organizador	Criação da possibilidade de produção de música (financeira e tecnicamente). Ir ao encontro da oferta (música) e da procura (compradores) através da combinação de autores de música. Acrescentar valor ao conteúdo através de uma combinação entre a reorganização e avaliação Promoção da música e outros produtos relacionados.
Vendedor	Promotor, Distribuidor	Comercialização de música para os consumidores.

Tabela G.1 Actores e os seus papéis na cadeia de valor

O mercado da música está a mover-se do seu modelo de negócios tradicional para novos modelos de negócio. Apesar das vendas de CDs serem ainda muito fortes, as editoras discográficas investigam desde já cenários de distribuição digital e tentam posicionar-se para proteger a sua actual quota de mercado nos mercados da música do futuro. Apesar desta mudança se fazer com alguma relutância por parte das editoras discográficas, uma vez que nenhum dos actuais modelos de negócios provou ser bem sucedido, é no entanto importante como resposta às perdas de lucros causados pela pirataria [OCBMS00].

Nos últimos anos, a pirataria de música aumentou significativamente em volume, principalmente devido ao crescente interesse por parte dos consumidores no formato MP3. Este formato, que codifica o áudio num

formato digital comprimido num tamanho razoável e com qualidade de CD, ganhou tremenda popularidade como forma de distribuir áudio através da Internet, criando ficheiros facilmente copiáveis. Apesar de alguns dos *sites* de MP3 terem sido encerrados pelas grandes editoras discográficas através de acções legais, o poder de distribuição da Internet tem-se relevado como imparável e fez com que as editoras discográficas começassem a pensar em cenários alternativos que sejam menos sensíveis à pirataria [OCBMS00].

A mudança gradual do mercado é aparente (Figura G.3): a distribuição física de música será substituída numa primeira fase por uma distribuição semi-física (por exemplo, descarregamento de formatos físicos), e depois por um modelo de distribuição completamente digital directamente para os consumidores nas suas casas [OCTRADR02].

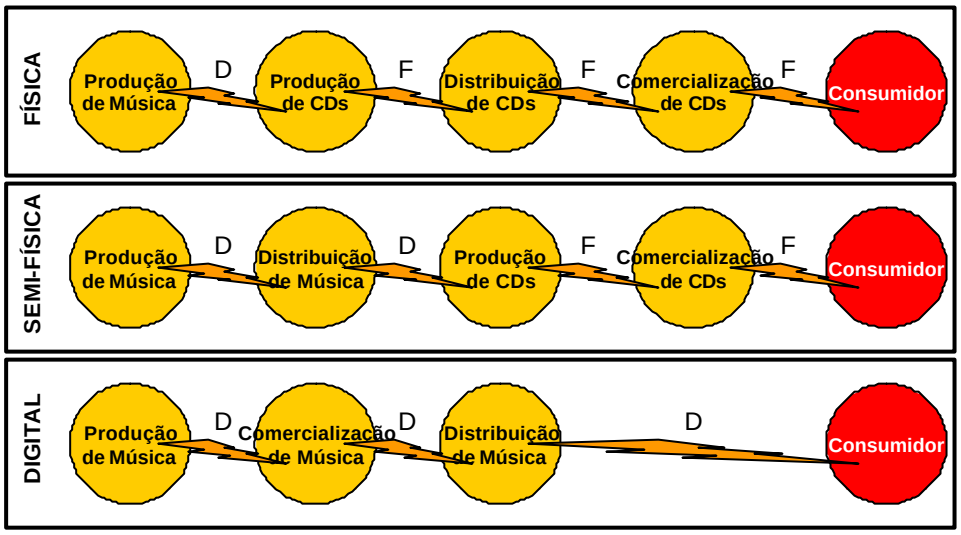


Figura G.3 Mudança gradual do mercado da música: Da distribuição Física (F) para a distribuição totalmente Digital (D)

No modelo de distribuição física, a música é produzida digitalmente, gravada para um meio físico e distribuída fisicamente e comercializada. Esta é a forma de comercialização actual da música. No modelo de distribuição semi-física, a música não apenas é produzida mas igualmente distribuída digitalmente, e depois escrita num meio físico numa loja de comercialização de música (por exemplo, o caso da iniciativa Sony/*Digital-On-Demand*). O último modelo de distribuição é totalmente digital: a produção de música é imediatamente seguida pela sua comercialização (pagamento primeiro, descarregamento da música depois), que depois pode ser distribuída, isto é, descarregamento do álbum pelo consumidor. Neste modelo, o requisito para efectuar reproduções físicas da música é removido da cadeia de valor [OCBMS00, OCTRADR02].

Modelos de Distribuição de Música Digital

Modelo de Descarregamento (Download)

Este modelo é baseado no modelo de distribuição tradicional e é o equivalente digital da actual forma de comercialização de música. Este modelo permite que os actuais papéis dos actores se mantenham na cadeia de valor, o que faz deste bastante apetecível e como tal dos primeiros a ser implementado e experimentado.

Neste modelo, dois actores estão posicionados entre o autor e o consumidor, tal como no modelo tradicional. O autor entra em contacto com a editora discográfica que processa a música e a grava. A loja *on-line* tem a função de substituir a editora discográfica para que o consumidor a editora associada a um artista. Isto possui duas vantagens [OCBMS00, DMPP01]:

- Os utilizadores não estão restringidos pelos stocks existentes e podem aceder a qualquer faixa de música lançada pela editora em qualquer altura (pelo menos em teoria);
- A quebra de stocks deixa de ser um problema uma vez que a oferta é ilimitada. Mais, o vendedor não precisa de tomar decisões acerca da música que tem que encomendar à editora, limitando-se a encomendar aquilo que o utilizador deseja.

O vendedor também deve gerir as relações com o consumidor (pagamento, serviço ao cliente, infra-estrutura, etc.). A música é descarregada em formato digital pelo utilizador, que paga ao vendedor por isso. Como resultado, o utilizador comprou a faixa musical que lhe foi entregue de forma digital (Figura G.4).

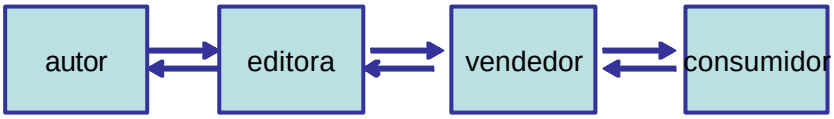


Figura G.4 O modelo de descarregamento

O modelo de descarregamento é comercialmente viável principalmente por uma razão: é muito parecido com o modelo tradicional. No entanto para o consumidor, este modelo é viável se este não tiver que efectuar o descarregamento da mesma faixa de cada vez que adiciona ou muda de dispositivos áudio [IPMF00].

O estabelecimento do preço da música obtida segundo este modelo pode ser realizada de diferentes formas, por exemplo:

- Pagamento por faixa;
- Pagamento por dimensão (MB);
- Pagamento por subscrição;
- Combinação dos elementos acima indicados.

Modelo de Fluxo Contínuo ou *Streaming*

Este modelo difere do anterior na forma técnica como a distribuição da música é realizada, que não é baseada no descarregamento da faixa de música por inteiro antes de ser escutada, mas sim em fluxo contínuo em tempo real da mesma para o utilizador através da Internet. A vantagem deste modelo em relação ao anterior é que o utilizador não tem que ter a cópia física da música de cada vez que deseja ouvi-la em dispositivos diferentes: pode fazer o descarregamento contínuo das faixas de música a partir qualquer sítio da Internet [OCBMS00].

O artista oferece a música a uma editora discográfica, que a produz. A editora, coloca a música num servidor próprio, que não está directamente acessível ao utilizador. Sempre que este deseja comprar uma música, acede a um portal na Web e procura a música através de um motor de pesquisa, capaz de procurar em servidores de outras editoras (Figura G.5). Quando a faixa musical é encontrada é descarregada para uma

directoria específica do utilizador no portal de Web permitindo que este possa efectuar descarregamento contínuo da mesma para um dispositivo sempre que deseje através de uma ligação à Internet [OCBMS00, OCTRADR02].

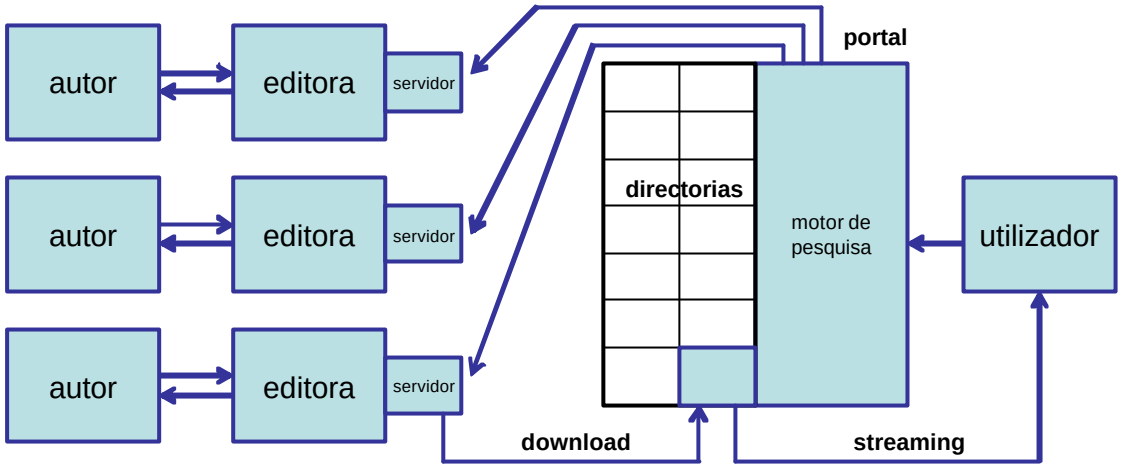


Figura G.5 O modelo de Fluxo Contínuo

Este modelo apresenta mais vantagens para os utilizadores que mudam frequentemente de local pois podem facilmente aceder à música sempre que desejarem em qualquer lugar onde estejam. Outra vantagem para os utilizadores é que não têm que recorrer a muitos *sites* Web à procura de música, estando esta agregada num único portal.

Uma vantagem para o editor e para o responsável do portal é que este modelo permite que os perfis de utilizadores sejam facilmente criados e geridos, uma vez que o utilizador deve poder aceder ao portal de cada vez que deseje ouvir uma determinada faixa musical. Como resultado, lucros podem ser gerados por publicidade na directoria pessoal do utilizador no portal [OCPH00, OCBMS00].

Uma grande desvantagem deste modelo é que a rede pode ficar congestionada pela técnica de fluxo contínuo utilizada. Por isso o portal deve garantir que a rede está bem dimensionada para satisfazer as necessidades dos utilizadores [TVOC00].

O estabelecimento do preço da música obtida segundo este modelo pode ser realizada de diferentes, por exemplo:

- Pagamento por faixa musical descarregada, da editora para a directoria no portal de Web;
- Pagamento por dimensão (MB), da editora para a directoria do portal de Web;
- Pagamento por cada faixa musical que o utilizador faça descarregamento contínuo do portal para o seu dispositivo;
- Pagamento por dimensão (MB), da directoria no portal para o dispositivo do utilizador;
- Pagamento por tempo (segundos), dependendo do momento do dia;
- Pagamento por subscrição mensal, anual, etc.;
- Pagamento por capacidade de armazenamento (MB) na directoria do portal;
- Combinações dos elementos acima indicados.

Modelo de Super-distribuição

O modelo de super-distribuição utiliza as redes sociais que existem entre os diversos utilizadores. Permite aos utilizadores a cópia e o envio de faixas musicais à sua família, amigos, vizinhos entre outros. Em termos comerciais, é muito interessante, uma vez que a divulgação de boca em boca, é na maior parte das vezes uma motivação mais forte para comprar e usar do que a publicidade normal. O modelo de super-distribuição utiliza tanto as capacidades de distribuição como de promoção dos utilizadores, também designado como o efeito '*Tupperware*' [TCFMI00].

Uma vez que os utilizadores tendem para distribuir as músicas que gostam a outros com os mesmos gostos musicais, aparecem oportunidades para criar comunidades de certos estilos musicais ou grupos, o que faz com que o modelo de super-distribuição floresça. Estas comunidades são particularmente apetecíveis para direccionar publicidade mais facilmente [TCFMI00, DMPP01].

Neste modelo os artistas oferecem a música ao super-distribuidor (editora), que gere um *site* de Web com diversos géneros musicais (comunidades). Depois da música ter sido revista e aceite, o super-distribuidor selecciona um número de "super-utilizadores" da sua base de dados que recebem um novo álbum ou faixa musical (Figura G.6). Estes são na verdade consumidores normais que são escolhidos para rever, publicitar e distribuir música a outros utilizadores.

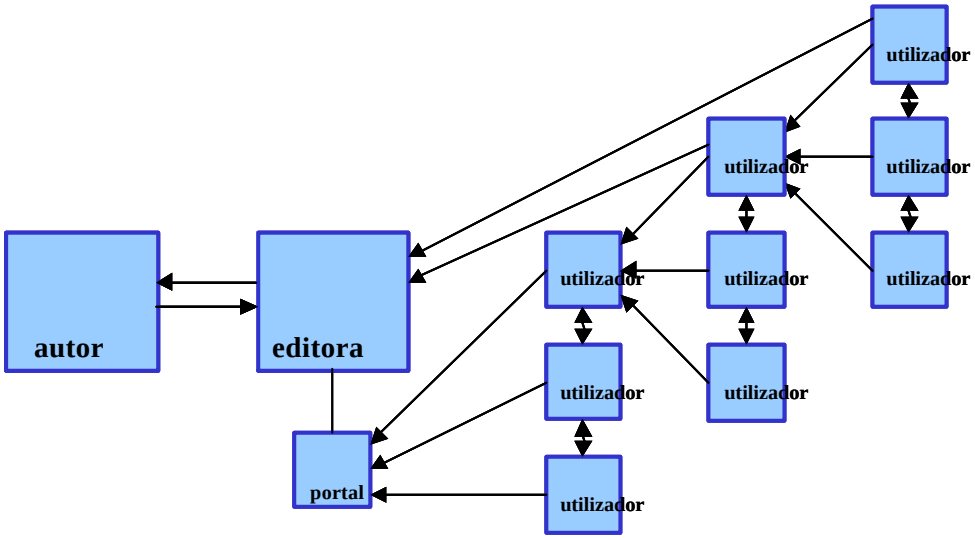


Figura G.6 Modelo de Super-Distribuição

No modelo de super-distribuição, o papel de distribuição da editora tende a desaparecer uma vez que a distribuição é efectuada pelos super-consumidores ou através da comunidade. No entanto, este modelo é bastante interessante para a editora uma vez que lhe permite efectuar acções de publicidade mais direccionadas para as comunidades de utilizadores. Outra vantagem diz respeito ao facto que a editora não precisa de se preocupar com a distribuição [OCBMS00].

Neste modelo o utilizador adquire uma faixa de música de outro utilizador em vez de o fazer à editora ou vendedor, embora o pagamento seja realizado para uma editora ou uma entidade financeira de confiança, que se encarregam de partilhar os lucros com o autor.

Modelo Directo

A ideia principal do modelo directo é a de que o artista constrói o seu próprio portal que é acedido directamente pelo utilizador. Desta forma os actores intermediários (editora e vendedor) não estão presentes neste modelo, uma vez que os seus papéis são desempenhados pelo autor. Os lucros destes são direccionados para o autor [OCBMS00].

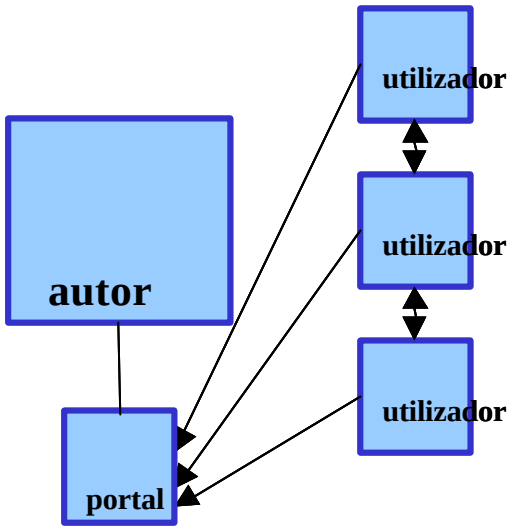


Figura G.7 Modelo Directo

Este modelo é muito semelhante em termos de requisitos de viabilidade ao de descarregamento e de fluxo contínuo. Um outro requisito deste modelo é que o artista deve ser bastante conhecido de forma a cativar utilizadores ao seu portal (Figura G.7).

De igual forma, as formas de estabelecimento de preço que eram aplicadas nos modelos de descarregamento e de fluxo contínuo são aplicadas aqui.

ANEXO H – IMPLEMENTAÇÃO DO SISTEMA OPENSDRM

Neste anexo encontra-se um CD-ROM que contém o código-fonte da implementação do sistema OpenSDRM. As instruções de instalação encontram-se no seu interior.

ÍNDICE REMISSIVO