Entrega Electrónica em Ambiente de Comércio Electrónico Seguro

Ilídio Chaves [1, 2]
lchaves@ipn.pt

Ricardo Simões [1]
ricardo@ipn.pt

Edmundo Monteiro [2]
edmundo@dei.uc.pt

[1] **Laboratório de Informática e Sistemas**
Instituto Pedro Nunes
Rua Pedro Nunes, Quinta da Nora
3030 Coimbra, Portugal
http://www.lis.ipn.pt

[2] **Laboratório de Comunicações e Telemática**
CISUC / DEI – Universidade de Coimbra
Pólo II, Pinhal de Marrocos
3030 Coimbra, Portugal
http://lct.dei.uc.pt

Resumo

O desenvolvimento de soluções de Comércio Electrónico do tipo B2C levou à automatização da maioria dos passos envolvidos no processo de compra, desde a busca de produtos (*procurement*) até ao pagamento.

Com a proliferação recente de produtos digitais, é agora possível conceber um ambiente completamente digital e automático com entrega imediata dos produtos ao cliente, imediatamente após a validação do pagamento. Neste cenário, o controlo dos direitos digitais e o uso de fortes medidas de segurança são cruciais.

Este artigo discute algumas técnicas de Gestão de Direitos Digitais (*Digital Rights Management* – DRM) e propõe duas soluções seguras para a entrega de produtos digitais ao cliente final.

Palavras-chave

Comércio Electrónico, Segurança, B2C, DRM

1. Introdução

Este artigo descreve um ambiente de comércio electrónico seguro, que suporta transacções comerciais num *Marketplace*. A plataforma proposta é dividida em vários componentes que foram desenvolvidos independentemente (módulos), tendo em conta os interfaces inter-modulares.

O tópico principal gira em torno do módulo de entrega electrónica, que é o passo final numa relação *Business-to-Consumer* (B2C). Considerando produtos físicos, as transacções terminam tipicamente com uma notificação, factura e número de encomenda, que são enviados para os clientes e gestores de negócio encarregues de processar a encomenda e enviar os produtos usando meios tradicionais (por exemplo correios). Já no domínio electrónico, o caso é bastante diferente. A oportunidade de construir um ambiente completamente automático, desde a pesquisa, passando pela encomenda e terminando na entrega é uma realidade, no entanto, a complexidade do sistema é muito superior. Neste cenário, a segurança é uma preocupação de relevo e alguns aspectos essenciais devem ser considerados:

- Os direitos de acesso a cada produto digital devem ser controlados;
- O processo de entrega electrónica deve ser rápido e eficiente, mas seguro.

Na próxima secção, a plataforma de comércio electrónico proposta é descrita. Na secção 3, são tecidas considerações sobre produtos digitais. As técnicas para a gestão de direitos digitais (DRM), usadas por esta plataforma, são descritas na secção 4. Finalmente, na secção 5, são propostas duas soluções diferentes para a entrega electrónica segura, que são depois comparadas na secção 6. As conclusões e considerações finais são objecto da última secção.

2. Componentes da plataforma de comércio electrónico

A Figura 1 ilustra a arquitectura geral da plataforma de comércio electrónico proposta. Esta é disposta em camadas com as entidades externas a interagir com o sistema através de interfaces específicos.

O sistema é concebido de tal forma que a programação de cada módulo é independente e segue normas emergentes.

A segurança é uma preocupação essencial no sistema, seja em cada um dos módulos ou na comunicação entre entidades.

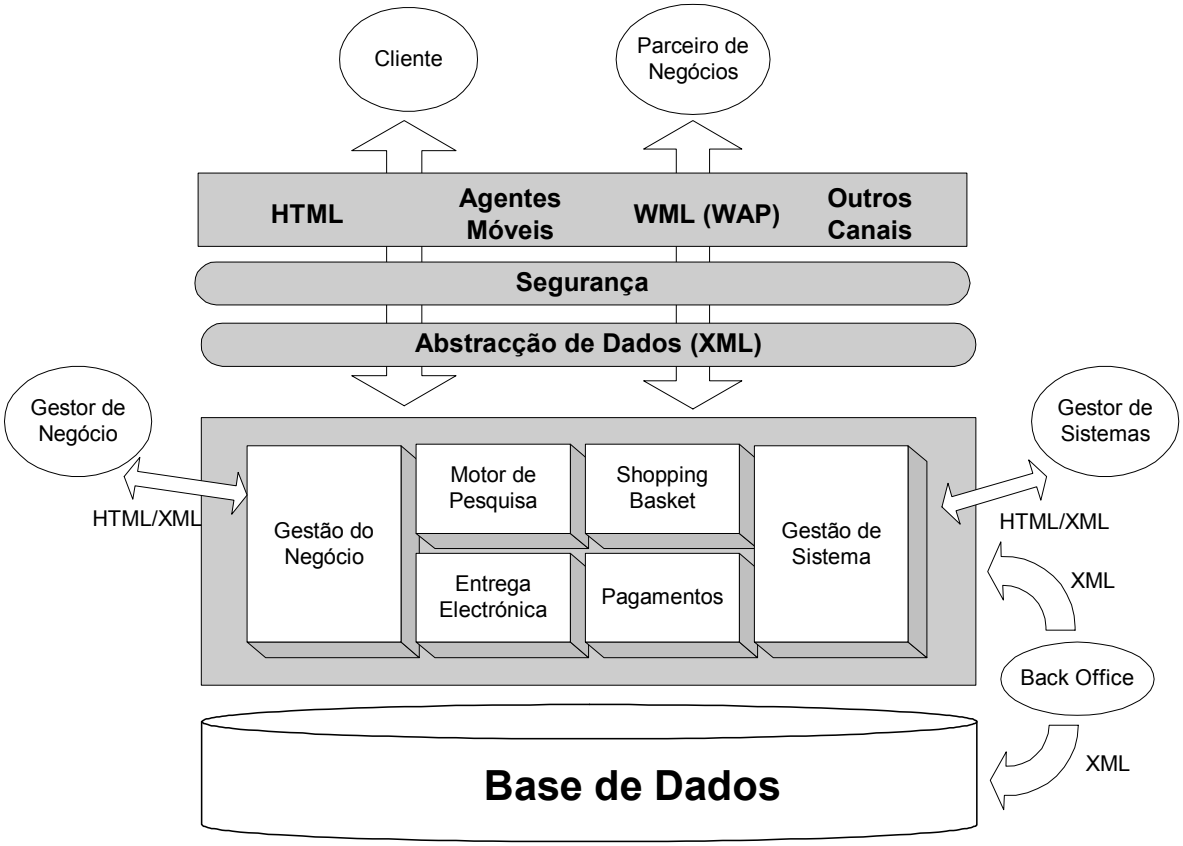

Figura 1 – Componentes do sistema de comércio electrónico proposto.

Uma descrição mais detalhada do sistema, com uma aplicação prática, pode ser encontrada em [1].

3. Produtos digitais e requisitos de segurança associados

Estamos de facto a viver num Mundo digital em constante crescimento. Muitos produtos podem agora ser encontrados em formato digital, poupando, na maioria dos casos, tempo e dinheiro. Documentos são um caso típico: a distribuição e venda de normas é um dos casos práticos da plataforma apresentada na secção anterior [2]. Outro caso de aplicação corrente, pode ser encontrado no domínio dos *E-Books*. Seguem-se mais exemplos de produtos digitais:

- *software*;
- música;
- filmes;
- outros produtos multimédia.

Numa infra-estrutura de comércio electrónico, a entrega de produtos digitais implica uma preocupação muito maior ao nível dos mecanismos de segurança. Antes de mais, os direitos de usar cada produto devem ser controlados. Estes direitos devem ser agregados aos produtos (no formato de concessões ou licenças, por exemplo) e definidos em cada passo do fluxo que faz parte do processo de produção e distribuição. Este é o objecto de discussão do próximo capítulo.

Tendo em conta estas considerações, os requisitos de segurança envolvem:

- *Autenticação* – que garante que as identidades das entidades envolvidas em cada transacção são conhecidas. O uso de *username/password* e PKI são soluções típicas.
- *Privacidade* – que garante que os dados são transmitidos com segurança e não são interceptados por terceiros. O uso de SSL é uma solução típica.
- *Integridade* – que garante que a informação não é alterada durante a transmissão. Assinaturas digitais e SSL são soluções típicas.
- *Não-repúdio* – para evitar a negação de transacções por alguma das entidades envolvidas. Assinaturas digitais e monitorização de tráfego são soluções típicas.
- *Controlo de Duplicação* – para evitar a distribuição não autorizada de produtos. Técnicas de atribuição de marca de água (*watermarking*) adquirem um especial relevo neste caso.
- *Gestão de Licenças* – para controlar o acesso e uso de produtos após a fase de compra. O utilizador deve apenas conseguir usar o equivalente àquilo que realmente pagou.

4. Gestão de Direitos Digitais

Considerando o ciclo de vida de produtos digitais e a sua distribuição, é assumido que a gestão de direitos [3] deve existir em todas as fases do processo de distribuição, desde o autor até ao cliente final.

A Figura 2 descreve os passos envolvidos na gestão de direitos digitais, começando no criador, passando pelo publicador e distribuidor e terminando no consumidor. O DRM age em cada passo do processo.

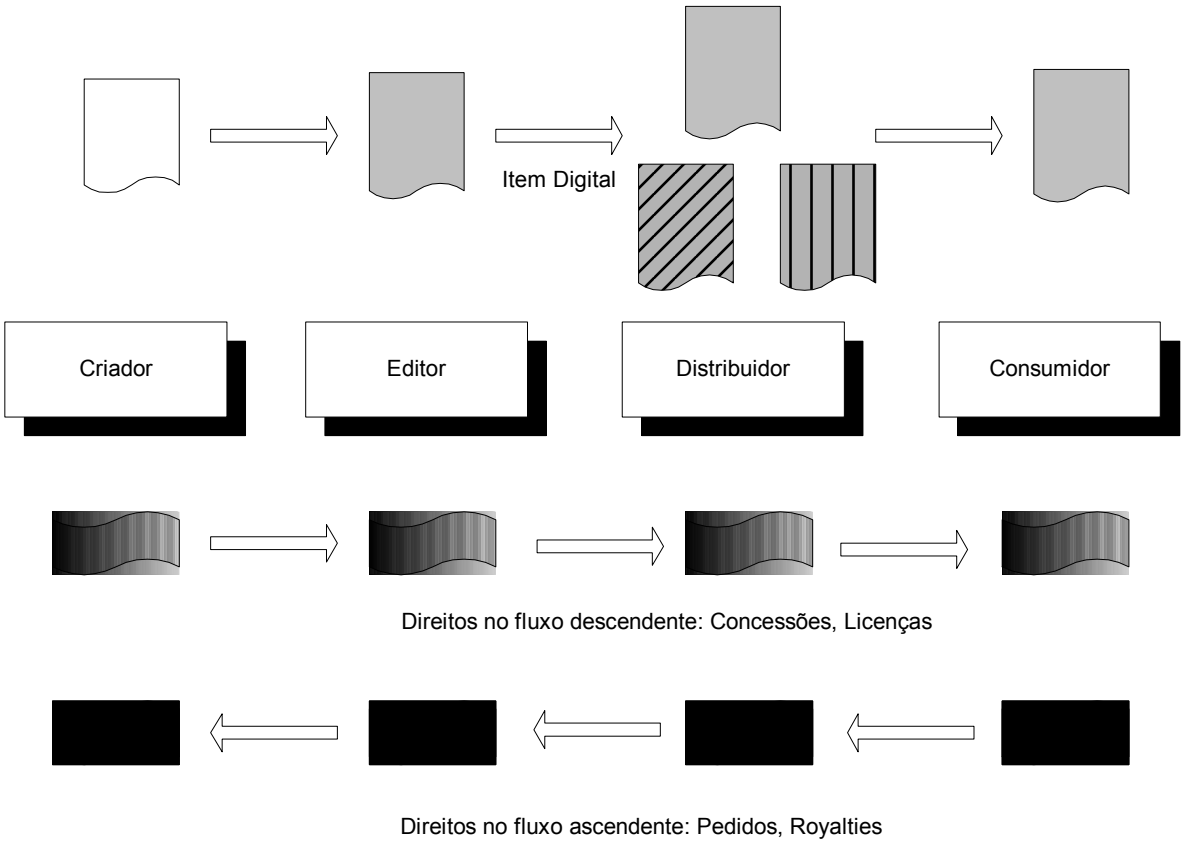

Figura 2 – Modelo multi-camada de gestão de direitos digitais.

A gestão de direitos digitais pode revelar-se muito complexa, dependendo do conteúdo e profundidade do fluxo de DRM. Por exemplo, um utilizador pode ter uma licença para copiar uma faixa musical indefinidamente ou um documento interno de uma empresa pode conter direitos que respeitam a posição hierárquica de um determinado empregado (administrador, gestor, etc.). Para além disto, as expressões que definem direitos, tornam-se ainda mais complexas quando se tenta imitar a situação homóloga física, contendo todos os intermediários envolvidos.

As técnicas de gestão de direitos digitais foram objecto de um considerável desenvolvimento no passado recente e várias organizações e empresas produtoras de *software* já propuseram algumas soluções. Para a solução de comércio electrónico proposta neste artigo, as soluções seguintes foram integradas:

- *XrML (extensible Rights Markup Language)* [4] - basedo em XML, define uma gramática para especificar direitos e condições para controlar o acesso ao conteúdo digital e serviços.
- *Adobe Portable Document Format* [5] – as versões mais recentes incluem encriptação RSA de 40 *bits* e a possibilidade de definir uma chave mestra para a criação e actualização de ficheiros e outra chave para a leitura. O autor do documento, pode

definir quatro tipos de operação: cópia de conteúdos, impressão, actualização e edição de notas e formulários.

- *Electronic Book Exchange System* [6] – O sistema EBX define um procedimento no qual livros electrónicos (*E-Books*) são distribuídos dos editores para os distribuidores e revendedores, dos revendedores para os consumidores, entre consumidores e entre consumidores e livrarias. Descreve os requisitos básicos para dispositivos de leitura electrónica e para os próprios livros electrónicos. Descreve também a forma como estes componentes "de confiança" interagem para formar um sistema compreensivo de protecção de direitos de autor que protege a propriedade intelectual dos autores e editores, e descreve também os requisitos dos consumidores. O modelo descreve também, de uma forma geral, a forma como os produtos e receitas para os mesmos são geradas e geridas.
- *Mpeg 21 Multimedia Framework* [7] – O objectivo do *Movie-Picture Expert Group* é o de criar normas que regulam os produtos digitais, desde imagens até à televisão digital. A gestão de direitos digitais é também uma preocupação fundamental deste grupo, que está a definir uma linguagem que exprime a gestão e protecção de direitos e propriedade intelectual (IPMP – *Intellectual Property Management and Protection*), disponível na norma MPEG4.
- *Windows Media Rights Management* [8] – A *Microsoft* propôs uma proposta ligeiramente diferente para a gestão de direitos digitais de objectos multimédia. Enquanto que, em outras soluções, a informação relativa a DRM é incluída no próprio ficheiro, em WDRM o conteúdo é encriptado e protegido contra uso ilegal através da emissão de uma licença específica. A gestão destas licenças é proposta na arquitectura geral descrita em [8].

5. Módulo de Entrega Electrónica do sistema de Comércio Electrónico proposto

Para a entrega electrónica, são descritos e comparados dois cenários que tomam conta dos aspectos de segurança necessários para a transmissão segura de produtos digitais ao cliente final.

Ambas as alternativas seguem uma aproximação diferente no que diz respeito aos mecanismos de segurança envolvidos.

5.1. Cópia de ficheiros para a área privada do utilizador

Nesta solução, cada ficheiro que passa pela gestão de direitos digitais é copiado para a área privada do utilizador que o adquiriu. Esta área é protegida por um mecanismo de *username/password* ou então por um sistema de autenticação baseado em certificados digitais, cuja gestão é assegurada por uma infra-estrutura PKI. O sistema sabe sempre o estado de cada encomenda, que poderá ser: *pendente*, *parcialmente completa* ou *completa*. Neste último caso, o sistema deixa a área activa durante um intervalo de tempo (que é um parâmetro configurável), durante o qual o cliente pode ainda obter os produtos digitais, por *download* directo (usando SSL para cumprir os requisitos de segurança) ou *email* (usando S/MIME para cumprir os requisitos de segurança). Após este período, a directoria é limpa para optimizar o espaço disponível no servidor de ficheiros, apesar de se manter o registo de todas as transacções efectuadas. A Figura 3 ilustra este caso.

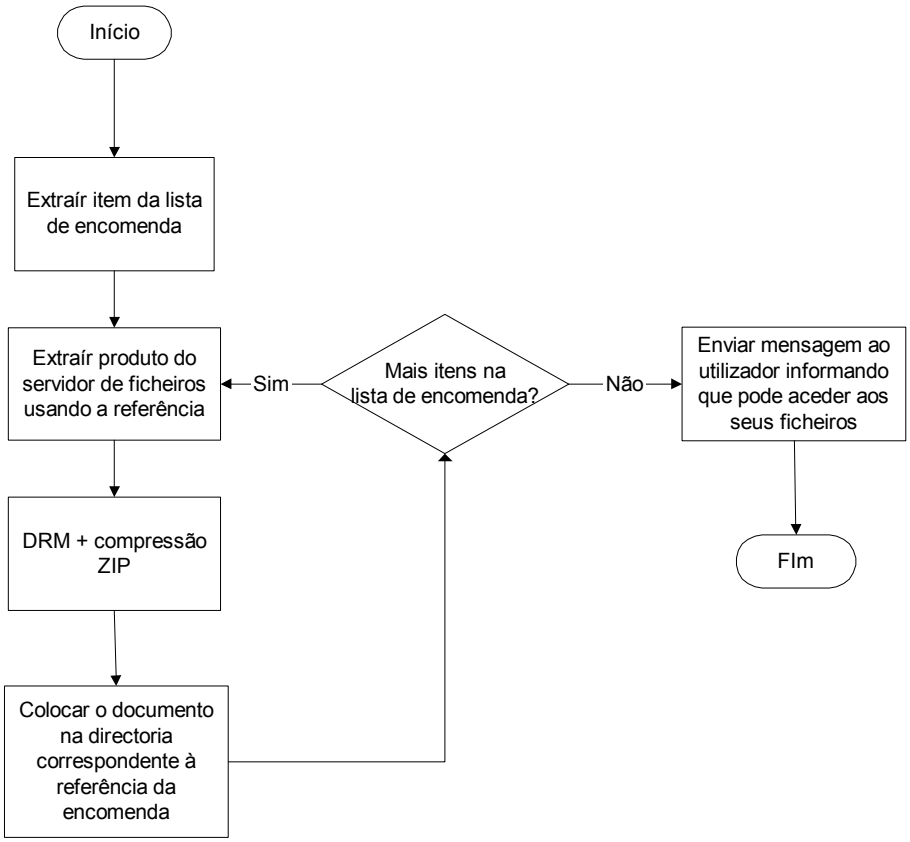

Figura 3 – Entrega electrónica com cópia dos ficheiros para a área privada do cliente.

A gestão de direitos digitais é aplicada antes da cópia dos ficheiros para a área privada. Para ficheiros *pdf* e de *media*, podem ainda ser aplicadas marcas de água de antemão. A compressão Zip é opcional e útil para optimizar o tempo de transmissão através da rede.

5.2 Uso de ponteiros encriptados para ficheiros

Nesta solução, a área de conteúdos encontra-se numa directoria comum (servidor de ficheiros), que não está acessível através de um ponteiro público. Para cada ficheiro, que é resultado do processo de gestão de direitos digitais, um URL encriptado é gerado usando um algoritmo bidireccional com uma chave única. Para este caso, os algoritmos RC4 da RSA (*stream oriented*) e o de *Rijndael* [1] (*block oriented*) [9] foram usados.

A chave usada para a encriptação dos URLs é diferente para cada utilizador e pode ter vários tamanhos, com o máximo de 2048 *bits* para o RC4 e 256 *bits* para o *Rijndael* (embora teoricamente o algoritmo de *Rijndael* suporte chaves de qualquer tamanho múltiplo de 32). Esta chave é gerada na fase de registo dos utilizadores da plataforma de comércio electrónico. Note-se que muitos sistemas ainda usam RC4, apesar do facto de que o AES oferece melhor segurança, visto que é orientado a blocos e é fruto de um algoritmo bastante mais avançado.

Após o processo de gestão de direitos digitais e encriptação do URL, um ponteiro é exibido ao utilizador. O conteúdo deste ponteiro não é "legível", visto ser encriptado, e aponta fisicamente para uma página que irá processar o pedido e posteriormente entregar o ficheiro. Antes, porém, irá tratar dos direitos digitais de acordo com o tipo de conteúdo e direitos do utilizador em causa.

Quando o utilizador selecciona um ponteiro, dá-se início ao processo inverso, com a desencriptação do URL usando a chave do utilizador e verificando o identificador da sessão (*session id*). Esta verificação oferece protecção à situação onde que o utilizador deixa a sessão aberta antes de efectuar o *download* dos seus ficheiros. Se o tempo permitido para cada sessão (que é um parâmetro configurável no sistema) expirar, é pedido ao utilizador um novo *login*. Após autenticação, um novo URL encriptado é gerado. Note-se que a natureza desta solução inibe o uso de gestores de *download* convencionais, o que permite controlar melhor todo o processo (*downloads* só são permitidos através do *browser*). Este cenário é apresentado na Figura 4.

---

[1] *O algoritmo de* Rijndael *foi eleito como o Advanced Encryption Standard (AES), após comparações exaustivas de vários candidatos, que foram objectos de estudos especializados, tal, como aquele que se pode encontrar em [10].*

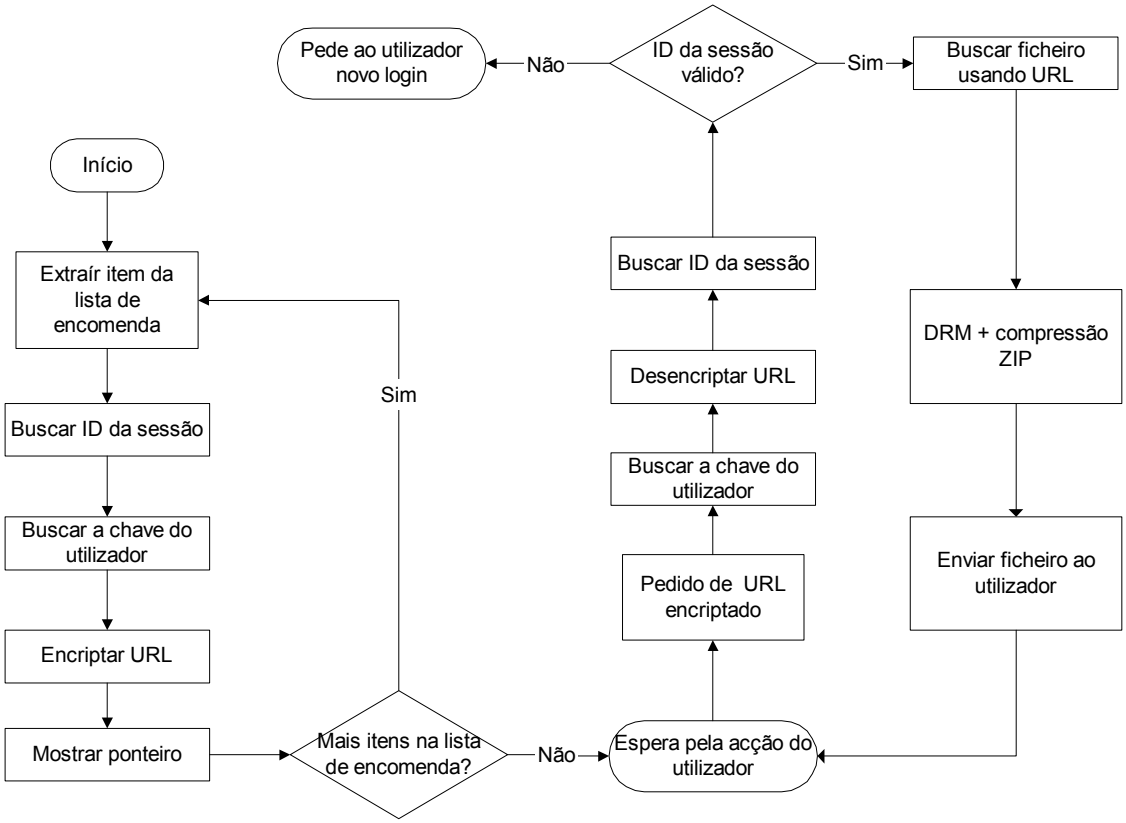

Figura 4 – Entrega electrónica com o uso de ponteiros encriptados

Para o não-repúdio na entrega, o modulo monitoriza a sessão de *download* e espera até que o bloco de informação é completamente enviado. Finalmente, os ficheiros temporários são removidos e o estado da encomenda é actualizado na base de dados.

6. Comparação das propostas apresentadas para a entrega de produtos digitais

Ambas as propostas apresentadas têm como objectivo fornecer um mecanismo de entregas digitais seguras para os utilizadores finais da plataforma de comércio electrónico. São fruto de diferentes soluções tecnológicas e aplicadas após a fase de gestão de direitos digitais.

A primeira solução é mais fácil de implementar. Divide o servidor de ficheiros em áreas de utilizador disjuntas, cada uma com o seu espaço reservado. Esta separação lógica tem, contudo, a desvantagem de utilizar mais recursos (espaço em disco). Para além disto, no segundo cenário, o expirar de uma determinada sessão leva à geração de novos URLs, enquanto que, no primeiro caso, o utilizador necessita de passar novamente pela fase de *login* mas os ponteiros físicos mantêm-se. Neste caso, não usar URLs encriptados significa que a origem dos ficheiros é mais fácil de rastrear, apesar de serem usados componentes que tentam esconder estes ponteiros.

A maior desvantagem da segunda solução tem principalmente a ver com o *interface* visual do sistema. Visto que os URLs são encriptados, a caixa de diálogo de *download* proporá ao utilizador gravar para o seu disco um ficheiro com um nome ilegível, o que poderá levar a confusão por parte do cliente (visto que o ponteiro é encriptado os caracteres não fazem sentido). O nome do ficheiro que é copiado para o disco é, no entanto, claro e legível, contém o nome de origem e o utilizador poderá, ele próprio, definir um novo nome. Esta limitação será ultrapassada na próxima versão, com o desenvolvimento de um componente específico.

7. Conclusões

A entrega electrónica é o próximo passo no processo de relação entre empresas e consumidores onde mecanismos eficientes de pesquisa de produtos e pagamento já foram desenvolvidos e implementados. Neste novo cenário, a segurança torna-se ainda mais importante para controlar todo o processo automático de enviar o pacote electrónico ao utilizador final.

A gestão de direitos digitais foi desenvolvida de forma a permitir que o utilizador opere sobre o produto em condições que dizem respeito directamente ao que efectivamente pagou. As técnicas de gestão de direitos digitais variam dependendo no tipo de produto electrónico, mas devem ser apresentadas ao utilizador de uma forma transparente para que não o confundam ou o tornem hesitante a mover-se para este novo ambiente completamente digital.

A entrega electrónica segura garante que os produtos electrónicos adquiridos, que já passaram pela fase de gestão de direitos, são entregues univocamente ao utilizador pretendido. Neste artigo, duas soluções foram apresentadas e comparadas, tendo em conta os requisitos de segurança necessários para por em prática os objectivos pretendidos.

Agradecimentos

Trabalho parcialmente financiado pelo Ministério da Ciência e Tecnologia através de uma Bolsa de Doutoramento no âmbito do programa PRAXIS XXI.

Referências

[1] I. Chaves, H. Martins, E. Monteiro, F. Boavida – "A Secure E-Commerce Platform to Enable the Worldwide use of Standards", Proceedings of 1er Congreso Iberoamericano de Seguridad Informatica, Morelia Michoacán, Mexico, 18-22 February, 2002.

[2] S. Downe, I. Chaves - "Progress Towards Web-Based Electronic Committees in the CEN/INES project (Internet Network for European Standardization)", SIIT'99 Proceedings, pp. 231-235, Aachen, September 15-17, 1999.

[3] F. Hartung, F. Ramme, "Digital Rights Management and Watermarking of Multimedia Content for M-Commerce Applications", IEEE Communications Magazine, November 2000.

[4] Content Guard, "eXtensible Rights Markup Language (XrML) 2.0, available at http://www.xrml.org

[5] Adobe, "Adobe Portable Document Format", http://www.adobe.com/products/acrobat/adobepdf.html

[6] The EBX Working group, http://www.ebxwg.org

[7] J. Lacy, N. Rump, P. Kudumakis, "MPEG-4 Intellectual Property Management and Protection (IPMP). Overview and Applications", MPEG doc, ISO/IEC JTC1/SC29/WG11/N2614, December 1998.

[8] Windows Media Rights Manager Documentation, available at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wmrm/htm/windowsmediarightsmanagersdk7.asp

[9] J. Daemon, V. Rijmen, "AES proposal: Rijndael", NIST AES proposal, June 1998.

[10] B. Schneierand, D. Whiting, "A Performance Comparison of the Five AES Finalists", Proceedings of the Third AES Candidate Conference, April 2000, pp. 123-135.