Electronic Delivery under a Secure E-Commerce Environment

Ilidio Chaves[1], Ricardo Simões[2], Edmundo Monteiro[3]

[1] **Laboratório de Informática e Sistemas** Instituto Pedro Nunes
Rua Pedro Nunes, Quinta da Nora
3030 Coimbra, Portugal

Laboratório de Comunicações e Telemática
CISUC / DEI – Universidade de Coimbra
Pólo II, Pinhal de Marrocos
3030 Coimbra, Portugal
ichaves@ipn.pt
http://www.lis.ipn.pt

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

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

Keywords: E-Commerce, DRM, Security, Encryption

Abstract. The development of B2C E-Commerce has led to automation in most steps of the purchasing process, from procurement to payment. With the proliferation of digital products it is now possible to consider a fully digital and automatic environment, with immediate delivery of the products to the customer, immediately after payment has been cleared. In this scenario, the control of digital rights and the usage of tight security mechanisms for delivery are crucial. This paper discusses Digital Rights Management techniques and proposes two secure approaches for Digital Product Delivery of purchased electronic goods to the end user.

Introduction

This paper describes a secure E-Commerce environment that supports commercial transactions of an internet marketplace. The proposed platform is divided into several components that have been developed separately (modules), taking into account the interfaces between modules.

This paper focuses mainly on the electronic delivery module, which is the final step in a business to consumer relationship. While, when considering physical products, the transactions typically end with a notification, invoice and order number, sent to customers and managers, the case is much different when considering digital products. The opportunity to build a complete automatic environment, from search, going through the order and ending at delivery, is a reality, but the complexity of the system is much higher. Security is a major issue in this scenario and several important aspects should be considered:

- Access rights to each digital product should be controlled
- The electronic delivery procedure should be fast and efficient but secure

In the next section, the proposed E-Commerce platform is described. In section 3, considerations are made about digital products. The Digital Rights Management (DRM) techniques used for this platform are described in section 4. Finally, in section 5, two different

approaches for secure electronic delivery are proposed and then compared in section 6. Conclusions and final considerations are object of the last section.

The E-Commerce platform components. Figure 1 illustrates the general architecture of the proposed E-Commerce platform. It is represented as a layered architecture with the external entities interacting with the system through specific interfaces.

The system has been devised in a way that programming of each module is independent and interfaces follow emerging standards.

Security is a major concern of this system, be it in each one of the modules or in the communication between entities.

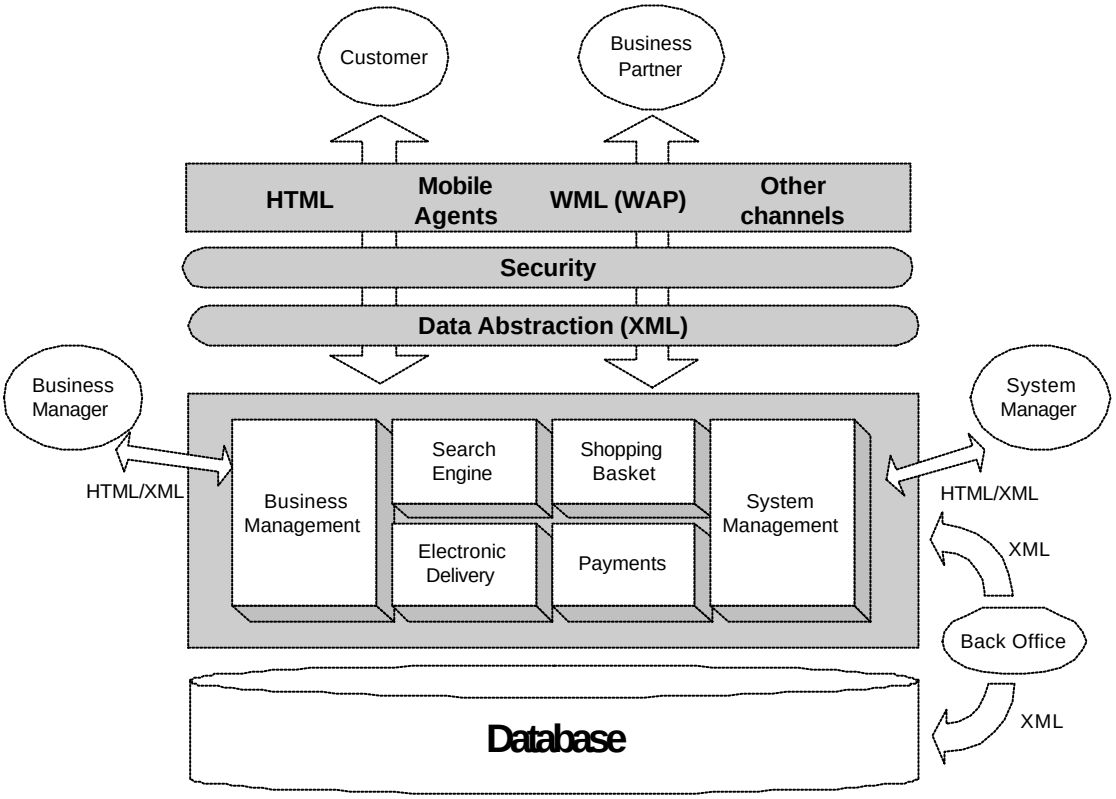

Fig. 1 – Components of the proposed E-Commerce System

A more detailed description of this system, with a practical use case can be found at [1].

Digital Products and security requirements. We are in fact living in an ever-growing digital world. Many products are now possible to find in digital format, saving in most cases time and money. Documents are a typical practical application: the distribution and selling of standards is one practical use case of the platform described in the previous section [2]. Another case is E-Books. Other typical digital products could be:

- software;
- music;
- movies;
- other multimedia products.

In an electronic commerce infrastructure, delivering electronic products entails a much stronger need of security mechanisms. First of all, the rights to use each product must be controlled. These rights much be attached to the products (in the form of grants or licenses, for example) and defined at every step of the product flow. This is detailed in the following chapter.

Taking into account these considerations, the security requirements involve:

- *Authentication* – that guarantees the identities of parties involved in a transaction. Username/Password and PKI are typical solutions.
- *Privacy* – that guarantees that the data is safely transmitted and not intercepted. SSL is a typical solution.
- *Integrity* – that guarantees that the information is not changed during transmission. Encryption and digital certificates are typical solutions.
- *Non-repudiation* – to avoid denial of transactions. Digital certificates and traffic monitoring are typical solutions.
- *Duplication Control* – to avoid unauthorized distribution of products. Watermarking techniques assume an important role in this case.
- *Licence Management* – to control access and usage of products after the purchase phase. The user should only be able to use what he actually paid for.

Digital Rights Management. Considering the life cycle of digital contents and their distribution, it is assumed that DRM [3] should exist in every stage of the distribution process, from the author until the end user. Figure 2 describes the stages of DRM for digital contents, beginning at the creator, passing through the publisher and distributor and ending at the consumer. DRM acts on each stage of the process.

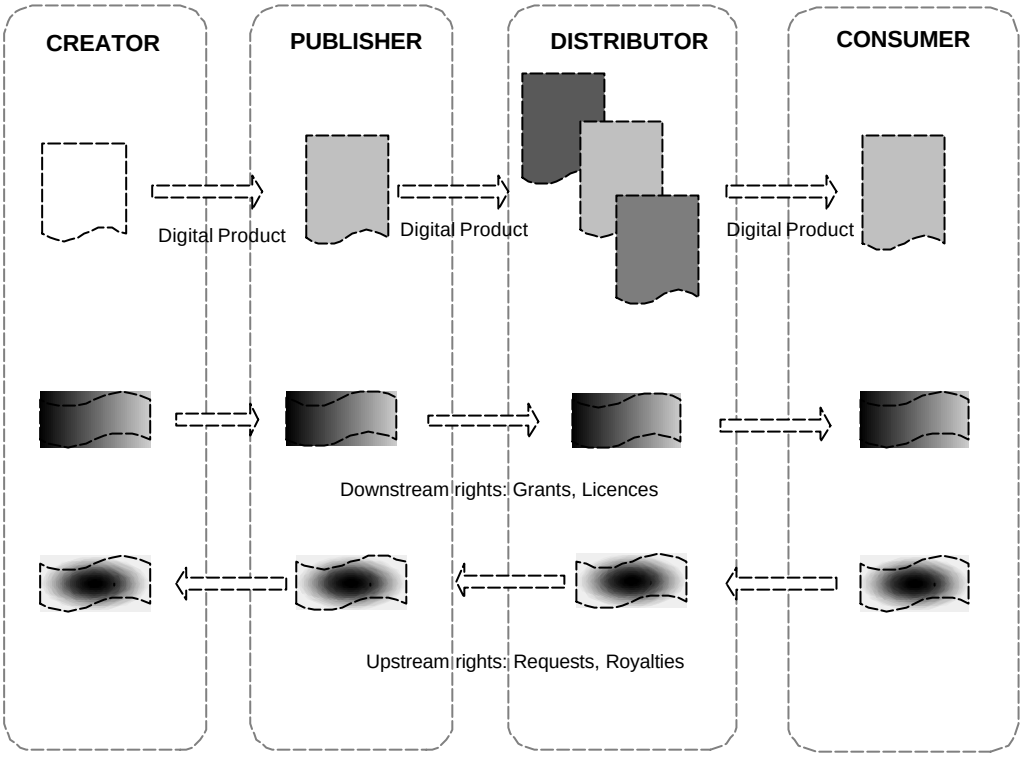

Fig. 2 – DRM multitier model

Managing DRM could be quite complex, depending on content and the length of the DRM flow. For example, a user could have a license to copy a music track indefinitely or an internal document of a company may define rights according to an employee's position (administrator, manager, etc.). Moreover, the expressions that define rights become more complex when trying to mimic the physical counterpart, which contains all of the intermediaries and distributors.

DRM techniques have evolved considerably in the near past and several organizations and software companies have already proposed some solutions. For the E-Commerce platform that is described in this paper, the following solutions have been integrated:

- *XrML (extensible Rights Markup Language)* [4] - based on XML, it defines a grammar for specifying rights and conditions to control the access to digital content and services.
- *Adobe Portable Document Format* [5] - latest versions include RSA 40 bit encryption and the possibility of defining a master key for the creation and update of files and another key for file reading. The author of the document may define four types of operation: content copy, print, update and edition of notes and forms.
- *Electronic Book Exchange System* [6] - The EBX system defines a way in which electronic books (e-books) are distributed from publishers to booksellers and distributors, from booksellers to consumers, between consumers and between consumers and libraries. It describes the basic requirements of electronic book

reading devices and the electronic books themselves. It also describes how these 'trusted' components interact to form a comprehensive copyright protection system that both protects the intellectual property of authors and publishers as well as describes the capabilities required by consumers. In addition, the model describes in general how products and revenue for those products are generated and managed.

- *Mpeg 21 Multimedia Framework* [7] - The aim of the *Movie-Picture Expert Group* is to create standards that regulate multimedia products that may range from images to digital TV. DRM is also a major concern of this group that is also defining a language to express rights and intellectual property management and protection (IPMP), available on MPEG4.
- *Windows Media Rights Management* [8] - *Microsoft* proposed a slightly different approach to DRM of multimedia objects. While, on other approaches, DRM information is included in the file, in WMRM the content is encrypted and protected against illegal usage by issuing a specific *licence*. The management of these licenses is proposed in the general framework, which is described in [8].

Electronic Delivery Module of the E-Commerce System. For electronic delivery, two scenarios, that handle the security aspects needed for the safe transmission of digital products, have been implemented and compared. Both alternatives follow a different security approach:

A. Copy of files to the user's private area

In this approach, every file that passes through the DRM stage is copied to the user's private area, which is protected by a username/password mechanism or a PKI infrastructure. The system knows the status of every order, which may be *pending*, *partially completed* or *fully completed*. In this last case, the system leaves the area active for an amount of time (that is a configurable parameter), during which the customer may still retrieve the products. After this period, the directory is deleted to optimise the space of the document server, although all transactions stay registered in the database. Figure 3 illustrates this case.

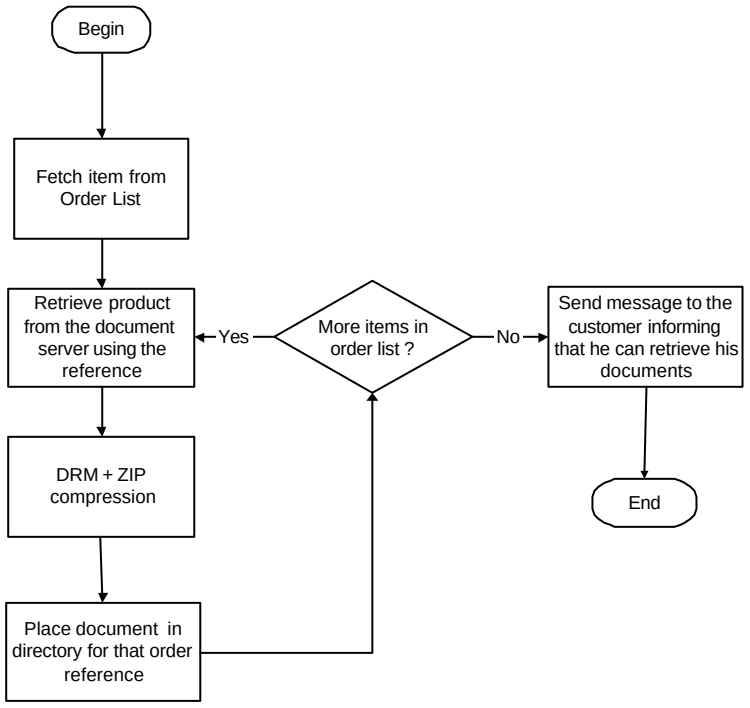

Fig. 3 – Electronic delivery, with copy of final files to the user's private area

DRM is processed before the file is placed in the user's private area. Also, for pdf and media files, watermarking may be applied beforehand. Zip compression is optional and useful to optimise transmission over the network.

B. Usage of encrypted links to files

In this approach, the content area is located in a common directory (document server), which is not accessible via a public link. For every file that is a result of the DRM process, an encrypted URL is generated with a bi-directional algorithm using a unique key. For this case, RSA's RC4 algorithm (stream oriented) and the *Rijndael* algorithm (block oriented) [9] have been used. The *Rijndael* algorithm has been selected as the *Advanced Encryption Standard* (AES), after comparing several alternative candidates, such as the study found in [10].

The encryption key used for encrypted URLs is different for each user and may have different sizes, with a maximum of 2048 bits for RC4 and 256 bits for *Rijndael*. This key is generated at user registration on the e-commerce platform. Many systems still use RC4, although AES offers better security, since it is block oriented and is a more advanced algorithm.

After the DRM process and URL encryption a link is displayed to the user. The content of the link is not "readable" since it is encrypted, and physically points to a page that will process the request and deliver the file. Previously, it will handle DRM according to content type and user rights.

When the user clicks on a link, the inverse process begins with URL decryption using the user's key and session id verification. This protects against the user leaving a session open before downloading his files. If the session time expires (which is a system configurable parameter) the user is prompted to login again. At this point a new encrypted URL is generated. Note that due to the nature of this approach, it is not possible to retrieve the files through conventional download managers, which entails a more controlled security environment (download is only possible through the browser). This scenario is depicted in figure 4.

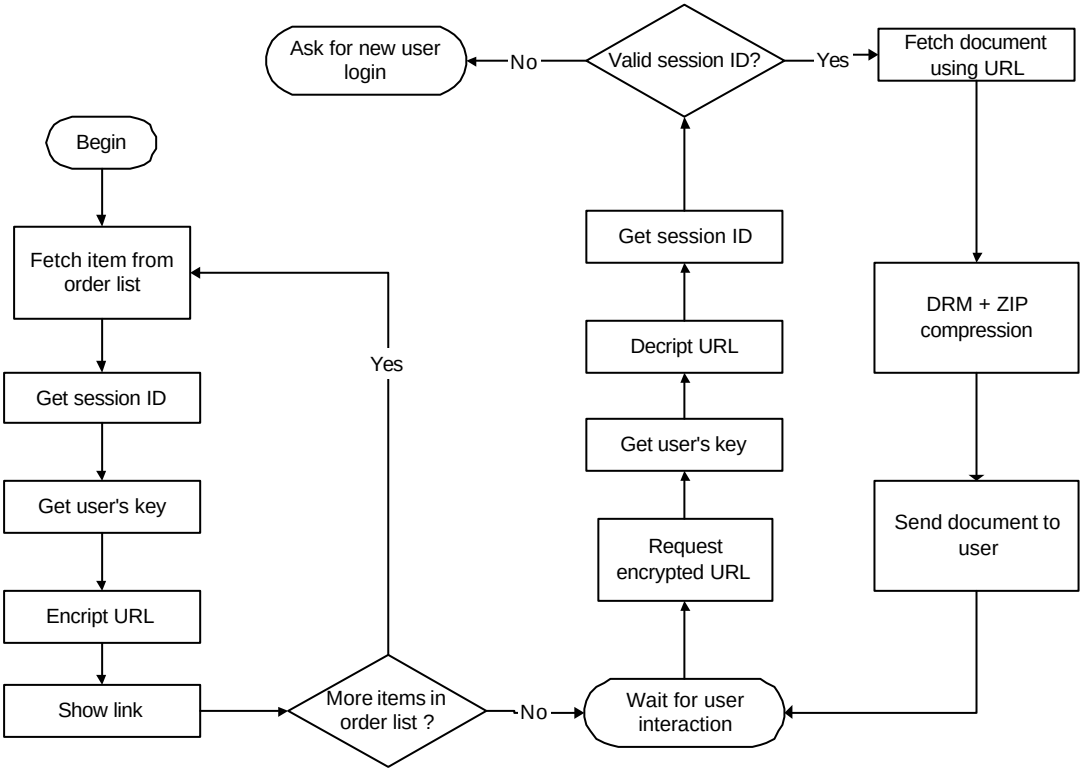

Fig. 4 - Electronic delivery with usage of encrypted links

For non-repudiation of delivery, the module monitors the download session and waits until the stream is completely sent. Afterwards, the temporary files are deleted and the order status is updated on the database.

Comparison between the proposed delivery scenarios. Both proposed scenarios aim to provide a safe delivery mechanism for end-users of the e-commerce platform. They convey different technological approaches and are both applied after the DRM phase.

The first approach is easier to implement. It divides the file server into separate user areas, each one having his own reserved space. This logical separation has the disadvantage however of using up more space. Also, in the second scenario, session timeouts lead to the generation of new URLs, while in the first case, the user must go through the login phase again but the physical pointers are the same. In this case, not using encrypted URLs means that the origin of the files is easier to trace, although components are used to hide these links.

The biggest drawback of the second approach has mainly to do with the visual interface of the system. Since the URLs are encrypted, the http download prompt will ask the user to save a file, with an unreadable name, which may introduce some confusion (because it's encrypted the characters don't make sense). The name of the file (on the "Save as…") dialogue is however clear and the user may change the name on download. On the next version, a specific download component will be developed to surpass this limitation.

Conclusions. Electronic delivery is the next step in business to consumer relationships, where efficient search and payment mechanisms have already been developed and implemented. In this case, security is even more important to control the whole automatic process of sending the electronic package to the end user. Digital Rights Management has been developed in order to let the user operate on each purchased item according to what he actually paid for. DRM techniques vary depending on the type of the electronic product, although they must be presented to the user in a transparent manner that won't lead him to confusion or make him hesitant to move to this total digital environment.

Secure electronic delivery assures that the purchased electronic items, which have already passed through the DRM phase, are delivered uniquely to the intended user. In this paper two approaches have been presented and compared, both taking into consideration strong security mechanisms.

References

[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.