Issues for the Commercial Distribution of Electronic Documents

Vassilis Prevelakis
Dimitri Konstantas
Jean-Henry Morin

University of Geneva
Centre Universitaire d'Informatique
Geneva, Switzerland

Abstract

This paper examines the issues surrounding the charging for the use of electronic documents. While traditional systems charge for the release of the document, we have adopted the approach of distributing intelligent documents (*agents*) that can initiate the billing procedure when the user wishes to view the document. We first present the requirements that should be met by a system responsible for the sale of electronic documents, followed by a presentation of our approach for meeting these requirements. Finally, we discuss how this mechanism will be used in the construction of the HyperNews system for the sale of electronic newspapers.

1 Introduction

Currently, the dominant medium of information distribution and dissemination is printed documents such as letters, books, newspapers, and magazines. However, over the last few years the volume of documents exchanged for private communications, or available for public access in electronic form [1][2][3][4][5] has increased exponentially. This is due to the fact that the majority of these documents, ranging from private letters to complete books, are directly created in electronic form using a computer editing system. Moreover, the wide availability of computer networks has allowed the faster and cheaper exchange of the electronic versions of these documents. Unfortunately, this new medium has so far resisted commercial exploitation. Apart from CD-ROM titles that are treated by the publishers as normal books, commercial document distributors, like book editors, newspaper publishers, and legal organisations are reluctant to distribute their documents in electronic form via the network.

This state of affairs can be explained if we compare the traditional commercialisation of printed documents with that of their electronic counter-parts. Printed documents, especially books, are inherently resistant to copying. Photocopying printed material is labour intensive and produces copies that are of inferior quality to the original. The removal of copyright notices and other alterations also involve a lot of effort and usually leave traces. By contrast, electronic documents can be modified, duplicated and distributed at virtually no cost. Thus, the control of ownership rights [6][7][8] is the reason for which commercial intellectual work rarely appears in electronic form.[1]

The aim of the MEDIA (Mobile Electronic Documents with Interacting Agents) project [12] is to develop the means that will allow the protection, commercialisation and dissemination of electronic documents under similar conditions as printed ones and, in addition, offer the reader of such documents all the advantages of electronic information processing technology [11]. Our approach in the MEDIA project differs from other approaches at the point of where the copyright control and payment of ownership rights are enforced. Traditional approaches [9][10] enforce the copyright control and payment at the point of the distribution of the electronic document delivering the raw document data. Our approach transfers the point of payment from the provider to the reader site, by encapsulating the data in a program (the agent), so that the copyright control and payment is enforced when reading the document and not when downloading it.

In this paper we describe the mechanisms and concepts of a system that enforces the copyright control and payment at the time the material is read. We also discuss the related issues and problems. We begin with a presentation of the requirements for the commercial distribution of electronic documents, followed by an overview of existing systems used for the commercial distribution of electronic documents. The next section includes a presentation of our system, while the last section presents our conclusions and future plans.

2 Requirements for the Commercial Distribution of Electronic Documents

It can be argued that a new medium warrants new thinking about possible commercialisation schemes. However, publishing is a mature industry and changes in the marketing and exploitation strategies are slow. Thus, while acknowledging that in the future, other styles and requirements will be developed according to the needs and ethics of the readers, we must, nevertheless, plan for situations that are similar to the existing (hard copy) distribution schemes.

This, in turn, implies that our system should attempt to accommodate the usage patterns of printed material. For example if a person purchases a book, then members of the same household should be able to read it as well. However, giving the book to a friend or colleague should deprive the original owner the right of accessing the book. The privacy of the readers should also be considered. For example, the copyright owner should be able to receive payment without knowing the identity of the reader.

In order to stay within the boundaries of the above framework, we must comply with the following requirements:

- The publisher should not need to keep information on the customer. Any person can purchase a book, or magazine without applying for registration with the publisher.

[1] Even CD-ROMs where the sheer mass of data has so far proven an effective disincentive for illicit copying are under threat because of the appearance in the market of low cost writable CD-ROM devices [13].

- Security. Assuming that the cost of individual items is relatively low, the security mechanisms should strike a compromise between robustness and usability. In other words breaking a single document should involve sufficient effort to discourage attacks. Moreover, although we cannot prevent text copying and screen dumps, we should not allow the copying of entire documents in one go.

- Capability for off-line reading of the material. To maintain the portability of the printed version, the electronic document should not be tied to a network connection.

- Various payment strategies should be accommodated by the system since each category of users may use different schemes to pay for their electronic material. For example, although significant effort has been expended, namely by Visa and MasterCard with the SET [21] specification, in order to achieve a common standard, it is most improbable that it will be the only electronic payment scheme. Other existing schemes like Millicent [14], NetBill [15], Digicash [16], CyberCash [17], NetChex [18], iKP [20] must also be taken into account.

- In order to maintain the analogy with printed versions of books or documents, we must ensure that once an electronic document is purchased, it can be read multiple times without additional payment. However, only the persons who have paid should be allowed access to the document. If a user hands over a document to a friend or colleague, the document would need to be purchased by the new reader as well.

3. Related work / Background

Electronic fund transfers and electronic data interchange (EDI) over financial and private networks have been around for some time now. These infrastructures are expensive and the Internet has paved the way for wide scale electronic commerce over open networks. But, many issues still need to be addressed before achieving this goal in a safe open and secure way. This section describes the background and the issues of electronic payment technologies over the Internet through existing systems in order to draw the requirements for our distributed document architecture.

In most electronic commerce systems there is a trade-off between efficiency, security and cost. In a general way, electronic commerce systems can be classified in different categories depending on how they deal with the following issues:

- Microtransactions : this issue is important specially in the scope of our work since we are dealing in information items whose cost may be as low as a few cents or even fractions of a cent. Credit card and similar payment systems are not suitable for such schemes since the transaction cost would be much higher than the amount to be paid.

- Security : the main concern of security is to provide, throughout the whole chain of the commercial transaction, the means to ensure the trustworthiness of all the parties. This usually involves the selection of authentication schemes, authorisation and also encryption of information. The level of security that will be selected depends on the severity of the perceived threat, the value of the exchanged information, etc. This level, in turn, determines key system characteristics such as key lengths, authentication devices (e.g. smart cards), etc.

- Anonymity : this issue faces the problem of hiding the customer’s identity in a way similar to the use of cash. Different techniques can be used like certified tokens, blind signatures, pseudonyms. Moreover, for low cost goods and every day transactions one might not want these transactions to be traceable for many reasons.

- Privacy and secrecy : this issue is more concerned by the protection of the content of information goods such as copyrighted documents and the privacy of users. It could also to some extent concern the aspect of certifying that the received document is conform to what has been sent.

- On-line and off-line payment models : On-line payment models refer to systems involving a third party during the commercial transaction for authentication and authorisation reasons. Whereas off-line payment models only involve the customer and the merchant. The first situation prevents easily problems of double spending and dishonest transactions. In the second situation, these problems could be solved by secure hardware components such as smartcards.

- Payment scheme : there are many different possible schemes depending on who creates the “electronic money”, when and how customers and merchants are debited or credited with real money, who initiates the commercial transaction.

- Repudiation of transactions and dispute handling: how the systems deal with these problems. What is the legal value of a digital signature etc.

The *Millicent* protocol [14] developed at the DEC SRC, is best suited for micropayments over the Internet (i.e. less than a cent). The model followed by this protocol is that of a trusted third party called a *broker* who’s role is to serve as an accounting intermediary between customers and merchants. A *scrip* is a piece of digital cash that is only valid between a given customers - merchant pair. Scrips are obtained from brokers which themselves obtain them from merchants. The scrip contains a value and when a customer makes a purchase with it, the amount of the sale is deducted from the scrip’s value and sent back to the customer as change. A scrip can be considered as an “account” between the customer and the merchant which is set up, used and closed. A scrip can not be spent more than once, can only be spent by it’s initial owner and at a specific merchant, has an expiration time and can be regenerated upon expiration. Different Millicent protocols offers various levels of security and privacy. Namely, *Scrip in the clear* offers no security and no privacy. The *private and secure* protocol uses a shared secret between the two parties to establish a secure communication channel. And the *secure without encryption* protocol does the same without the privacy aspect in order to achieve better performance.

The *NetBill* [15] system from Carnegie Mellon University is a set of protocols for micropayment of information goods on the Internet. It is composed of a set of protocols involving customers, merchants and a NetBill server (i.e. an account server which is linked to conventional financial institutions). This enables the aggregation of many small transactions in to larger transactions. In this model, the NetBill server acts as a trusted third party ensuring the atomicity of the transactions (i.e. payment and delivery of the information goods). There are three phases in a NetBill transaction. In the first phase, the customer requests a price offer for the desired item. At this stage a bid for that item can also be included as well as personal information in order to qualify for special prices (e.g. student ID, frequent buyer ID). The merchant replies with a price quote. The second phase is initiated by the customer acceptance. The encrypted information goods are then sent to the customer but the decryption key will only be sent after completion of the third phase, namely the payment. In this third phase, the customer sends a digitally signed payment order to the merchant. The merchant includes the decryption key to this order, digitally signs it and sends it to the NetBill server. Then, upon completion, the NetBill server sends back to the merchant a digitally signed receipt including the key. The merchant forwards a copy of it to the customer. The system allows also for easy use of pseudonyms for anonymity but in any case, the NetBill server knows both parties identity and transaction amounts. However, it can ignore everything about the content of the goods through simple encryption techniques.

The system developed by *Digicash* [16] relies on a software based electronic money system called *Ecash*. Both clients and merchants are given an Ecash software which can be thought of as an electronic wallet in which withdraws from a bank can be put in or deposits to a bank can be made to. The system relies on the bank who's role is to act as a back-end to the system to certify that the electronic payments are valid (i.e. that coin signatures are valid) and to serve both the customers and the merchants. The system allows also for person to person payments and for customer anonymity through "*blind signatures*".

The *CyberCash Secure Internet Payment Service* [17] is based on a metaphor of physical payment. Customers are given CyberCash Wallets. Merchants use the Secure Merchant Payment System (SMPS). The CyberCash Gateway Servers are operated by CyberCash and in the future by banks. This system relies on the use of existing financial networks which are totally independent of the Internet for communicating between the CyberCash Gateway Server and the banks or credit institutions. For the time being, it supports only credit cards. In the future, it will support electronic checks, electronic cash and micropayments. A transaction is initiated by a customer clicking on a merchants "PAY" button. This action generates an electronic order form at the merchants site which is sent to the customer. The browser opens the CyberCash wallet window thus allowing the customer to select a payment instrument (credit card). Upon confirmation of the amount by the customer, the information are sent encrypted to the merchant which appends his own identification information and passes the payment request to the CyberCash Gateway Server. After validation of the payment request an acceptance or denial information is sent back to the CyberCash Gateway Server which is forwarded to the customer as a digital receipt. The system uses 56 bit DES private-key to encrypt all the messages between wallets, merchants and CyberCash Gateway servers. The DES key, which is unique for each transaction, is then encrypted using RSA public key technology. The length of the key is currently 768 bit but 1024 bit has been approved by the United-States government and will be eventually. Finally, a digital signature is appended for source authentication and non-repudiation purposes. CyberCash is following the credit card institutions and will be compliant with the Secure Electronic Transaction specification (SET) [21] defined by the major credit card institutions namely Visa and MasterCard.

NetChex [18] is an electronic check system on the Internet. Consumers must be registered at the *Net 1 Inc.* A local software (Windows based) is responsible for secure communication with the NetChex system which then processes the transaction through traditional banking systems and networks. The issuer of a NetChex check is notified upon completion of the transaction by e-mail.

CAFE [19] (*Conditional Access For Europe*) is an ESPRIT project that developed a secure electronic payment system that protects the privacy of the user. It is based on smartcard technology for electronic wallets. These electronic wallets look like pocket calculators or PDAs (Personal Digital Assistants) in which smartcards are inserted. The system acts like a prepaid off-line payment system. Users have to “load” electronic money from an issuer prior to spending it at points of sales. The system is multi-currency and there is no need to contact an issuer or third party during a payment transaction. Communication between PDAs and other devices is made by an infrared channel.

The *Mondex* [24] system is also based on similar smart card technology. It follows the electronic cash wallet paradigm by storing the electronic cash on an encrypted microchip. The security scheme relies on a digital signature which is generated by the chip on the card. This digital signature can only be recognised by other Mondex enabled participants in a transaction. It has been designed to support multiple currencies (five) and to allow person to person transactions. Various trials and pilot have been undertaken involving banks (NatWest and Midland in the UK, Hong Kong Bank outside the UK) and British Telecom for the telephone infrastructure.

Internet Keyed Payment Protocol (*iKP*) [20] is a credit card based Internet payment system developed by IBM. It was part of the ACTS project SEMPER. It contributed in 1995 to MasterCard’s SEPP specification which led to MasterCard and Visa’s joint SET specification. The system relies on the following assumptions: both customers and merchants must have an existing relation with a financial institution. The customer must have a credit card. The merchant must have a contract with an acquirer accepting the client’s card. The system uses traditional encryption algorithms (i.e., RSA). The iKP system has three variants. In the *1KP* variant, only the acquirer has a public key. In *2KP*, both the acquirer and the merchant have public keys (i.e., both can sign). Finally in *3KP* all three parties have public keys.

The *Secure Electronic Transaction* (*SET*) [21] specification is the common standard that is developed by two of the major credit card institutions (Visa and MasterCard). This common effort is the result of an agreement which took place early in 1996. American Express has also announced that they would support the SET specification. Some of the major partners in this agreement include GTE, IBM, Microsoft, Netscape, SAIC, Terisa Systems, and Verisign. In the background of SET there are two competing individual efforts, namely SEPP for MasterCard and STT for Visa. The current specification does not account for microtransactions nor for smartcard technology. SET is based on both asymmetric (e.g., RSA public key can be used for digital signatures) and symmetric (e.g., DES) cryptography.

The *Java Electronic Commerce Framework* (*JECF*) [26] developed by JavaSoft is a promising solution for the integration of existing payment instruments such as credit (using the SET protocol) and debit cards, as well as emerging solutions like electronic cash, electronic checks and smartcard technology. The system will support microtransactions, frequent buyer style advantages, procurement cards, coupons, etc. Currently, the JECF API specification are available [27] while the final implementation is expected to be released sometime in 1997.

The overall feeling that prevails in the field of electronic commerce on open networks is that many proprietary protocols and trials have been set. Each one of them addressing some specific issues. There is a clear need for standards addressing all the issues and providing well defined requirements for API developers integrating in a unified way existing payment schemes and technologies. These standards should be flexible enough to allow easy integration of current and future payment schemes and technologies. For example smartcard technology in this field is still in it’s infancy but could be a promising solution for wide spread safe and secure electronic commerce in both networked and real world.

4 Method for the distribution of copyrighted documents.

In the design of our system we made the decision to package each document with the program that regulates access to the article. Each document is thus a separate *agent* that is responsible for the following tasks:

- Release information regarding the document(e.g. title, date, size etc.).
- Supervise the copying of the entire agent (serialisation).
- Communicate with a billing agent that must also be present in the same workstation. The purpose of the billing agent is to provide a single point of contact for all the other agents in the system that need to charge the user account.
- Control access to the document. The document is normally encrypted to prevent unauthorised access. The agent will handle the decryption in co-operation with the billing agent.

The main problem that the design is facing is to prevent the user from bypassing the agent security mechanisms and accessing the data component of the agent directly. If such attempt is successful then the charging mechanism will have been rendered inoperative. It should be noted that what we strive for is a system that will make it expensive to break the protection mechanism of an agent. The biggest risk, however, is generic failures. These would allow the user to devote significant effort to find a generic weakness in the system that would allow access to all the agents with small incremental effort.

Another consideration is the cost to the information provider if the system is compromised and the security procedures have to be changed. By encapsulating the security mechanism inside the agent, the information provider can alter the security policy easily without affecting the agents already deployed. Thus, compatibility constraints with the older versions will not be an issue. Since the user environment deals with the agents and does not take into account the way these agents work internally, multiple versions of the agents can be resident on the same machine without mutual interference.

Given those considerations we have opted for a modular architecture which is displayed in Figure 1. A key actor in this transaction is the credit institution which may be a bank, a credit card company, etc. The purpose of this institution is to act as a trusted party between the information provider (seller) and the user (client). Both seller and client trust the credit institution to authorise the unlocking of articles in exchange of money that is transferred from the user account to the account of the information provider. This scheme is based on public key encryption [25].

Under this scheme, article M is encrypted using conventional encryption and the key k is placed in the agent. To avoid the risk that the user may discover the key by searching through the code of the agent, we encrypt k using the public key of the credit institution (C), producing $E_C(k)$. An article identification string (AIS) containing additional information such as the cost of the article, the beneficiary of the transaction, article information for auditing and other statistical data, is appended to and signed by the information provider (using the provider's private key P). The result, $S_P(E_C(k)$, AIS), is then stored in the agent

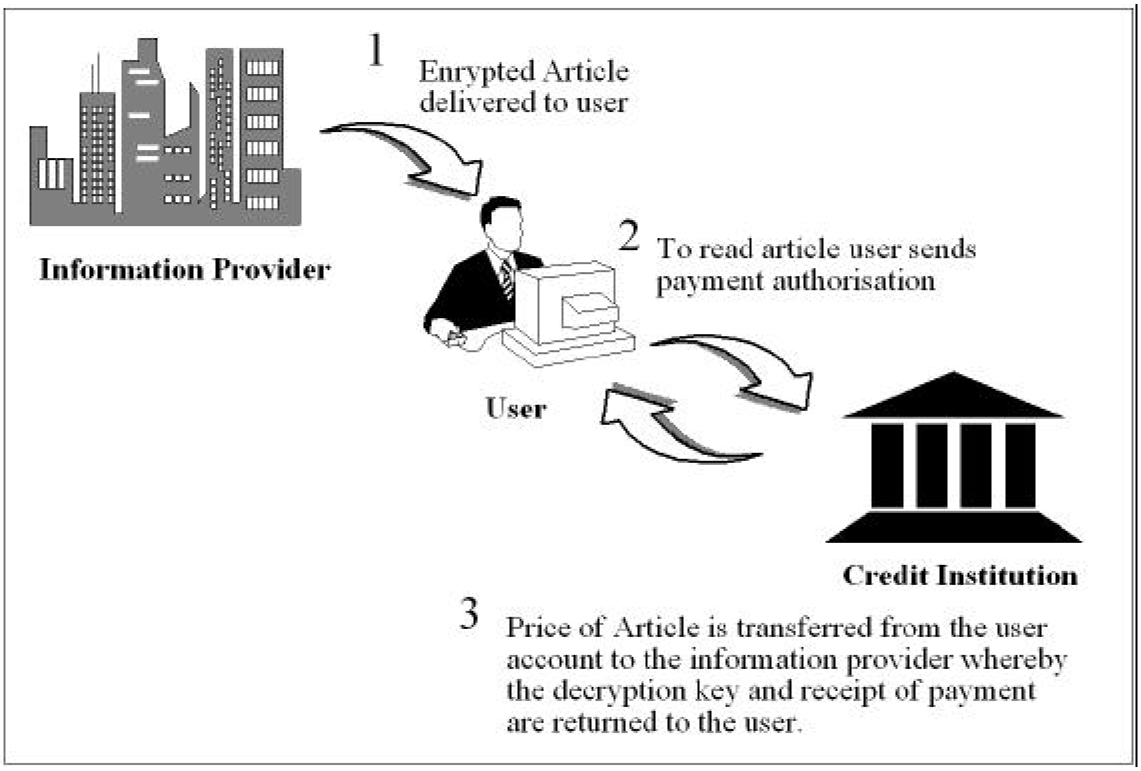
1
Enrypted Article delivered to user
Information Provider
2
To read article user sends payment authorisation
User
Credit Institution
3
Price of Article is transferred from the user account to the information provider whereby the decryption key and receipt of payment are returned to the user.

Figure 1: The exchange of an electronic document.

When the user wishes to unlock the article the agent will contact the credit institution and receive a special session key T encrypted with the user's public key ($E_U(T)$). The user will be able to decrypt $E_U(T)$, acquiring access to the key that will be used for the rest of the communication with the credit institution. $S_P(E_C(k)$, AIS) will be signed with the private key of the user (U) and the result is encrypted with the session key and sent directly to the credit institution.

The credit institution use the session key to decrypt the message:

$$D_T(E_T(S_U(S_P(E_C(k), \text{AIS})))) = S_U(S_P(E_C(k), \text{AIS}))$$

This will be validated using the user public key, giving:

$$V_U(S_U(S_P(E_C(k), \text{AIS})))) = S_P(E_C(k), \text{AIS})$$

From there we verify the signature of the information provider:

$$V_P(S_P(E_C(k), \text{AIS}))) = E_C(k), \text{AIS}$$

We now have the encrypted key for the article $E_C(k)$ and the article identification string (AIS). Since this information has been verified against the public key of the information provider we can be sure that they are valid.

At this stage an amount equal to the price of the article will be transferred from the user account to the account of the beneficiary. Then $E_C(k)$ will be decrypted using the credit institution private key and the article key k will be immediately encrypted using the session key that was received from the client, producing $E_T(k)$. In addition the credit provider will construct a receipt for that article so that the user will be able to have that article unlocked in the future.

The agent will receive $E_T(k)$ and decrypt it with the session key to get at k. At this stage the agent will be able to decrypt the article and display it on the screen. The basic mechanism can be used to implement different charging policies so that the user be offered a price range depending on whether the article will be viewed, printed, or whether audio or video components should also be unlocked and so on (Figure 2).

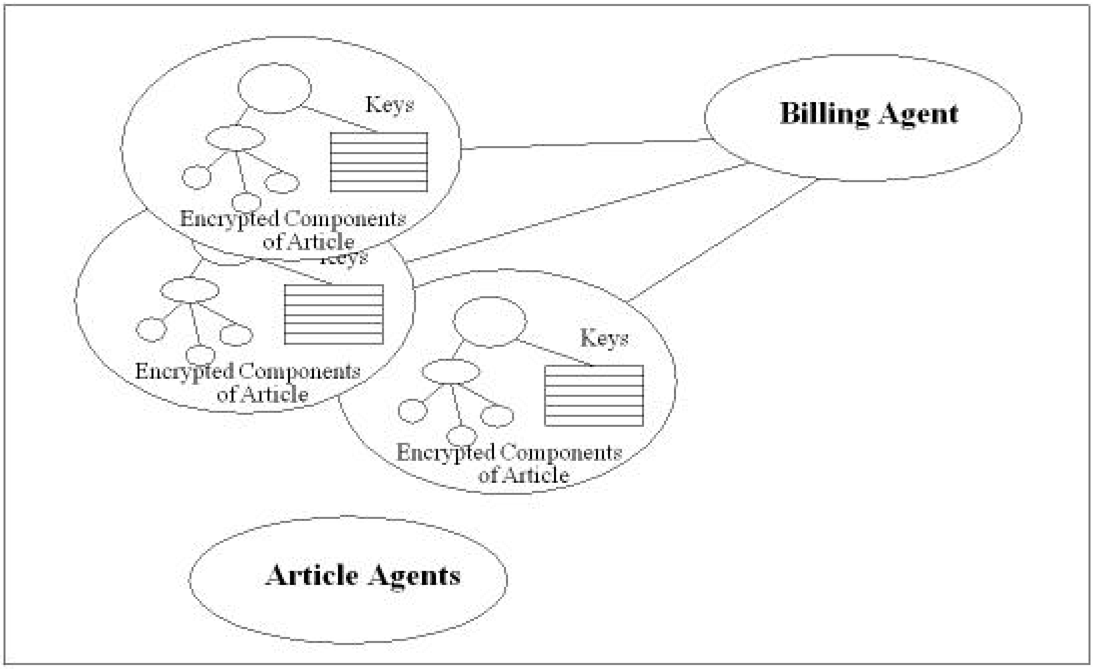
Keys
Encrypted Components of Article
Keys
Encrypted Components of Article
Keys
Encrypted Components of Article
Billing Agent
Article Agents

Figure 2: Agents on the user workstation.

We mentioned earlier that the credit institution will hand a receipt as well as $E_T(k)$. This is so that the agent does not need to arrange for long-term safe keeping of the decryption key. If the agent is terminated (e.g. to make room for new material) the user can still retrieve the article and give the old receipt to the new agent and this should be sufficient for the article to be again unlocked.

To prevent these receipts from being copied by users and thus creating a back door to the agent payment system, we still require the receipt to be validated by a credit institution. Although the user, in principle, is responsible for the safe keeping of those receipts, by putting the credit institution in the loop we allow those receipts to be tightly tied to the user who purchased them. Under the scheme described below, only persons with access to the private key of the user will be able to use the receipt. In this case, the repeated use of the same receipt will alert the credit institution that a user account may have been compromised.

The receipt includes the identification of the article, the components that have been paid for, identification of the user who purchased the article, time stamps etc. This information is signed by the issuing credit institution and need not contain any hidden, or encrypted information.

The user wishing to unlock a paid article will hand the agent the receipt. The agent will append the receipt (r) to the $S_P(E_C(k)$, AIS) packet described above. This will be signed and encrypted as before and the resulting $E_T(S_U(S_P(E_C(k)$, AIS), r)) message sent to the credit institution. Note that if the various credit institutions have exchanged their public keys, the credit institution that processes the receipt need not be the one that issued it. Thus a user switching banks will still be able to use the receipts charged to the old account, provided that we have a unique identification scheme for the users. If this is not possible the user may arrange for the old credit institution to inform the new one of the old account number.

The validity of the receipt is checked against the following elements:

- The signature of the issuing credit institution validates the contents of the receipt.
- The request $E_T(S_U(S_P(E_C(k)$, AIS), r)) is signed by the user, so that we can compare the user identification code attached to the public key held by the credit institution with the user identification code embedded in the receipt.

If the two conditions are met we can be reasonably sure that the new request is valid and the credit institution will return just $E_T(k)$, since this time a receipt should not be issued.

4.1 Off-line operations

In the case where a user would like to be able to view the articles off-line, the role of the credit institution must be delegated to a proxy. This proxy can be a smart card that can perform public key encryption internally [22][23]. For example, the CAFE project [19] and the Mondex system [24] use the smart card technology for off-line transactions. The basic assumption is that the card should contain, but under no circumstances reveal, two private keys. The first will be the private key of the user and the other will be the private key of the credit institution.

Needless to say that if the second key is compromised then the entire system of distribution will be compromised. As such it is evidently quite important to ensure that the smart card technology chosen for this scheme ensures the non-disclosure of its contents.

The card will offer the following services:

- **Credit.** It will be “charged” with money from the user account at the credit institution during an on-line connection with this service. As articles are accessed while the user is off-line, charge is deducted from the card.
- **Article unlocking:** Since the card will have the private key of the credit institution it will be able to unlock articles using a scheme similar to the one used for the on-line connection.

- **Log of charged items.** Since the charging will be performed off-line a record must be kept of the prices of the articles accessed and the beneficiaries of these transactions. During the next “recharge” of the card this information will be uploaded to the credit institution and will be credited to the correct accounts. The problem of a user that does not recharge his card can arise but could be solved for example by having a deposit on the card (i.e., if the user stops using the card he will have an incentive to return it to get back the deposit. By return, we may mean that the user simply sticks the card into an ATM for example).

Depending on the capacity of the card and the frequency of the connections with the credit institution, the log may not fit in the card. In this case the card may be used to hold multiple credit lines from a number of information providers. Thus, credit is transferred from the user account to the accounts of the selected information providers at the time of the card “charging.” The disadvantage is that the user will not be able to transfer charge from one information provider to the next while being off-line.

Alternatively, there may be a single smart card operator responsible for the collection of all the fees, while providers are paid fixed rates, depending on statistical information or some other benchmark.

5 Conclusions

The mechanisms described above form the basis of a distribution scheme for an electronic newspaper under the HyperNews project. In this project a publisher of a traditional newspaper (L'Hebdo) will be releasing an electronic version to subscribers over the Internet. Each newspaper is broken up into individual articles and each one is stored in a separate agent.

For each user, special software creates a customised view of the newspaper that includes only the articles that match the user profile. Since the articles are independent, users pay only for the articles they choose to read.

The HyperNews project is expected to provide the necessary feedback and experience that will allow the mechanisms described in this paper to evolve and come closer to the needs of the users of the system. In addition, we expect to be able to evaluate possible weaknesses of the system with respect to security and privacy. More specifically we want to address issues like the following:

- Prove that the protocol used for the transactions is safe from replay attacks.

- Since the credit institution has access to the keys of all the articles, it is clear that it can also acquire access to all the data of the information providers.

- There is a need for mechanisms for accepting new credit institutions into the scheme. Under the current scheme, users will have to request fresh copies of all the articles that they wish to pay using the new credit institution.

- Agents arriving on the user system must be able to determine whether the execution platform that they are expected to use has been compromised. Otherwise a malicious user may be able to trick the document and/or billing agent into releasing the keys used for all the transactions.

References

[1] Tages Anzeiger, http://www.tages-anzeiger.ch/

[2] The Electronic Telegraph, http://www.telegraph.co.uk/

[3] The New-York Times, http://nytimesfax.com/

[4] Time magazine, http://www.pathfinder.com/

[5] L’Hebdo, Electronic journal, http://www.hebdo.ch/

[6] Pamela Samuelson, "Legally Speaking: Copyright and Digital Libraries", Communications of ACM, Vol. 38, No 4, April 1995

[7] J. Ebersole, “Protecting intellectual property rights on the information superhighways”, International Publishers Association Bulletin, Volume X, No. 3, 1994, pp. 3-43.

[8] John S. Erickson, “ A Copyright Management System for Networked Interactive Multimedia”, proceedings of *DAGS’95 Conference on Electronic Publishing and the Information Super Highway*, May 30-June 2,1995, Boston.

[9] Mind's Eye Electronic Publishers, http://mindseye.com/

[10] Steve B. Cousins, Steven P. Ketchpel et al, “InterPay: Managing Multiple Payment Mechanisms in Digital Libraries”, Proceedings of the *Conference on Digital Libraries*, 1995.

[11] Jean-HenryMorin and Dimitri Konstantas, “Towards Hypermedia Electronic Publishing”, Proceedings of *second IASTED/ISMM International Conference on Distributed Multimedia Systems and Applications*, Stanford, California, August 7-9 1995.

[12] Dimitri Konstantas, Jean-Henry Morin and Jan Vitek, “ MEDIA : A Platform for the Commercialization of Electronic Documents”, in *Object Applications*, Ed. Denis Tsichritzis, CUI, University of Geneva, 1996.

[13] Jason J. Hyon and Michael D. Martin, “ CD It for Yourself”, in *Byte*, Volume 21, Number 6, June 1996.

[14] S. Glassman, M. Manasse, M. Abadi, P. Gauthier, P. Sobalvarro, “*The Millicent Protocol for Inexpensive Electronic Commerce*”, *Fourth International World Wide Web Conference*, Boston, December 11-14, 1995.

[15] B. Cox, J.D. Tygar, M. Sibru, “*NetBill Security and Transaction Protocol*”, proceedings of *First Usenix Workshop on Electronic Commerce*, New-York, July 11-12, 1995

[16] D. Chaum, “*Achieving Electronic Privacy*”, Scientific American, August 1992, p. 96-101

[17] CyberCash, Inc., “*CyberCash White Papers*”, http://www.cybercash.com/cybercash/wp/whitepapers.html

[18] Net1, Inc., “*The NetChex system*”, http://www.netchex.com:80/

[19] J.-P. Boly, A. Bosselaers, R. Cramer, R. Michelsen, S. Mjolsnes, F. Muller, T. Pedersen, B. Pfitzmann, P. de Rooij, B. Schoenmakers, M. Schunter, L. Vallee, M. Waidner, “*The ESPRIT Project CAFE, High Security Digital Payment Systems*”, *Third European Symposium on Research in Computer Security*, LNCS 875, Springer-Verlag, Berlin 1994, p. 217-230

[20] IBM, “*Internet Keyed Payment Protocols (iKP)*”, http://www.zurich.ibm.ch/Technology/Security/extern/ecommerce/iKP.html

[21] VISA, MasterCard, "*Secure Electronic Transactions, New draft as of 8/7/96*", http://www.visa.com/cgi-bin/vee/sf/standard.htm, http://www.mastercard.com/set/set.html

[22] D. Naccache, D. M'Raihi, "Cryptographic Smart Cards", IEEE Micro, Volume 16, Number 3, June 1996.

[23] J.-F. Dhem, D. Veithen, J.-J. Quisquater, "SCALPS: Smart Card for Limited Payment Systems", IEEE Micro, Volume 16, Number 3, June 1996.

[24] Mondex, http://www.mondex.com/

[25] R. Rivest, A. Shamir, L. Adelman, " A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, volume 21, #2, February 1978, pp. 120-126

[26] Java Soft, "*White Paper: The Java Electronic Commerce Framework (JECF)*", http://www.javasoft.com/products/commerce/doc.white_paper.html

[27] Java Soft, "*Writing Code for the JECF*", http://www.javasoft.com/products/commerce/doc.writing_code.html