Special Articles on Multimedia Information Processing

Tamper-Resistant Charging Technology for a Seamless Environment

Hiroshi Aono, Reiko Hoshino and Sadayuki Hongo

Most music download services provided by mobile e-commerce impair the user convenience, because of protecting measure for illegal copy to prevent extracting the downloaded digital contents from the terminal. To solve this problem, we have developed a system that enables to redistribute music and other content freely while charging for the content.

1. Introduction

In recent years, digital content that has typically been provided in broadband Internet environments such as Asymmetric Digital Subscriber Line (ADSL) has also come to be distributed via mobile terminals. This development is essentially the result of faster Internet connections on cellular handsets. At the same time, illegal copying of digital content obtained from download services has become a major problem. The main means of solving this problem is to implement systems that either prevent copying or limit it. This approach, however, limits the terminals that can be used, which is a disadvantage for the user. On the other hand, allowing unrestrained distribution of digital content would make it difficult for Content Provider (CP) to collect usage fees.

Past methods proposed for preventing illegal copying include complete prohibition of copying [1] and the allowance of only primary copying (no copying of copies) [2][3]. Methods such as these have come to be adopted as illegal-copying-prevention technologies that assign unique IDs to media or devices. They have been implemented in a variety of systems including SD memory cards, DVD-R/RW, Content Protection for Recordable Media (CPRM), MagicGate[*1] memory sticks, and

*1 MagicGate is a copyright protection technology developed by Sony for multimedia data. It encrypts copyright-protected music and other data and enables playback and transmission of that data only on or between devices determined to be legitimate by an authentication process.

Blue-ray Disk. These technologies, however, make use of terminal-unique information to limit the use of content, and therefore have great potential for preventing the open distribution of digital content.

There is also the superdistribution model [4] and soft-denchi ("software battery") system [5][6] that aim to achieve open distribution of digital content by charging for content at the client side. The superdistribution model allows for unrestrained distribution of encrypted digital content by delivering and transferring licensing information including a content decoding key through the use of a secret key stored in tamper-resistant hardware called a "secure multimedia card", Keitai-de-Music ("Music on Your Mobile") [7] based on the superdistribution model, which is one example of a system that enables unrestrained distribution of digital content. The soft-denchi system enables to be charged for at the client side when software is used. In this process, a soft-denchi manager decreases the amount of previously purchased (prepaid) value whenever the software comes to be used. The user can use the software until that amount reaches '0' and can always recharge the system with new value. Soft-denchi also features portability—it enables to be used at other terminals. This, however, requires to connect a soft-denchi management server via Internet.

In addition to the above, NTT DoCoMo, in collaboration with professor Tsutomu Matsumoto of Yokohama National University, is proposing a client-side charging system to enable the redistribution of digital content while collecting remuneration for its use [8]-[10]. It aims to accomplish this by performing charge processing in a manner inseparable from the playback of digital content. This system would enable content providers to collect usage fees even in the case of unrestrained distribution of content. Furthermore, by incorporating a charging system based on the proposed framework in content, the end user would have no need to change client software or hardware for different CP charging methods. This idea of charging for content usage on the client side is similar to the ideas of the superdistribution model and soft-denchi system. The main feature of the proposed system is that it prevents illegal playback and charging independently by performing charge computation inseparably and simultaneously with the playback of digital content while maintaining convenient services for end users.

This article first explains the preconditions and requirements of this service as well as attack scenarios, and then overviews the proposed model, data format, and associated player. Next, it describes an implementation of the proposed system, and finally reports on an evaluation of system safety and performance.

2. Client-Side Charging System by Inseparable Charge Computation from Content Playback

2.1 Basic System Configuration

Figure 1 shows the basic configuration of this system. The system of CP, fee-collecting agent, and end user.

CP first prepares content data (M) and by using data creation function which constructs charge logic (P) that shows the rules for charging to collect usage fees appropriately, and formats specialized content (data) that combines P and encrypted content M (M'). This data is downloaded via the network to the end user's specialized player, which computes usage fees simultaneously with data playback and pays the fee-collecting agent the fee for using M. The fee-collecting agent collects listening/viewing information with respect to M from the end user, and distributes sales proceeds based on that information to the CPs that have provided the user with content.

We point out here that no communications are performed with the CP or fee-collecting agent at the time of using content, which means that either a prepaid or postpaid scheme can be considered as a method for paying usage fees. Since the use of a postpaid system would require the study of a method for ensuring payment, we assumed the use of a prepaid system in the implementation presented here. Specifically, to give the system portability in an off-line state to satisfy the requirement that data can be used on any terminal, and to prevent illegal usage of that data, we adopted a system that stores a prepaid amount of usage fees and resulting listening/viewing information on a tamper-resistant smart card.

2.2 Service Requirements

If content playback and charge processing are performed independently of each other, there is a high possibility of illegal action such as the viewing or listening of content without paying usage fees and the collection of usage fees without playing back content. The inseparable performance of content playback and charge processing on the client enables CPs to collect their usage fees and end users to use content while paying each CP accordingly, both in a trouble-free manner. It also enables content to be distributed freely.

General requirements for setting up such a service can be

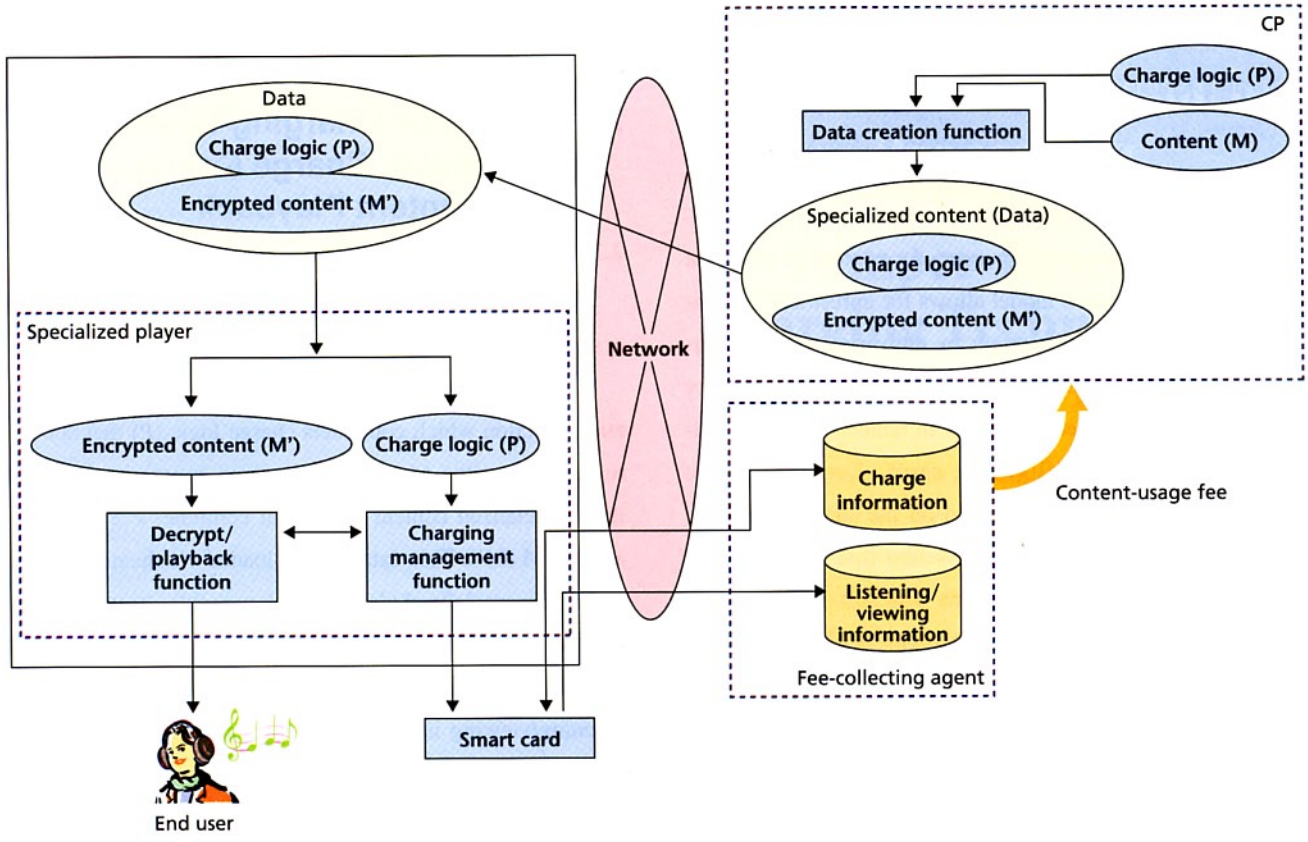

Figure 1 Basic system configuration

broadly divided into those on the CP side and those on the end-user side. These are described below.

1) CP-side requirements
- Charge processing must execute simultaneously with content playback.
- Charge settings can be modified on a content-by-content basis.
- Usage fees can be collected in proportion to content usage.

2) End-user requirements
- Content can be played back on execution of charge processing.
- Content can be used by any end user on any terminal by copying that content.
- Communicating with a CP or other entities at the time of playback is unnecessary.

2.3 Attack Scenarios

We examined attack scenarios for the basic system configuration shown in Fig. 1. The capabilities of attackers are assumed as follows.

- Observe data input/output between modules on the specialized player
- Alter input/output between modules on the specialized player
- Observe data within a module on the specialized player
- Alter data within a module on the specialized player
- Alter internal processing within a module on the specialized player
- Directly access the smart card

With these capabilities, an attacker has the potential of threatening the service requirements described above through the following scenarios.

1) Overwrite P to prevent correct charging
2) Observe illegally and record the key for decrypting M' into M to playback that content (extract M from downloaded data)
3) Save analog data generated at playback of M and redistribute that content
4) Directly access the smart card without executing data to alter prepaid money or charge information
5) Execute data without outputting correct results to the smart card
6) Playback content but change output to the smart card at a point between the specialized player and smart card without charge processing within the smart card
7) Intercept and falsify interaction between the smart card and fee-collecting agent

2.4 Proposed Model

The following describes the model proposed for the service requirements and countermeasures against the attack for the basic system configuration presented in Section 2.1. This model was designed under the following assumptions.

- The resistance of the smart card to tampering is reliable.
- Certification authorities are reliable.
- The specialized player is tamper resistant and secret information inside the smart card will not be uncovered by static analysis.
- Attack scenario No. 3 presented in Section 2.3 is outside the scope of this study.

The main elements of the proposed model are the same as those of the basic system configuration, but the specialized player is newly configured to incorporate measures for dealing with the service requirements and attack scenarios presented above. In more detail, the specialized player consists of specialized content (data), a signature-verification module (Verifier), a data-splitting module (Splitter), a content-playback module (Decoder), a control module (Manager), and a smart card (**Figure 2**). To prevent the extraction of M, data integrates charge logic P and encrypted content M' in an inseparable form. The Verifier checks to see whether data has been delivered from the correct server and whether it has been tampered with. This function is necessary to prevent the use of M' or P that might have been altered. The Splitter divides data into M' and P. The smart card, in turn, executes P, performs charge processing, and generates a key (k) for decrypting M'. Performing both charge processing and key generation on the smart card means that computational results obtained on the smart card are needed for content playback, and that illegal charging by executing only charge processing and illegal use of content by executing only key generation can be prevented. The Decoder consists of the Decrypt part that decrypts M' using k and the Decode part that plays back M. The Manager sends P to the smart card, passes k obtained from the smart card to Decoder, monitors whether P is being correctly executed on the smart card, and terminates playback if it is not correct. Furthermore, in the event that the decrypting of M' is not proceeding correctly, the Manger prevents charging from taking place (see Section 2.6, "Content playback procedure," for details).

2.5 Format of Specialized Content Data

Content data M is converted to specialized content (data) at a CP and played back at a specialized player. **Figure 3** shows the data format employed by this scheme.

In the figure, data is divided into n blocks (data = {$block_1$, $block_2$,..., $block_n$}) per charge unit. Each $block_i$ (i = 1,..., n) corresponds to the smallest unit for charging and consists of charge logic (P_i) describing the charging for that unit and content M_i' for that charge unit ($block_i$ = {P_i, M_i'}). For example, charge logic (P_i) might instruct the system to charge 5 yen for ten-seconds listening to or viewing that content, to give a 50% discount

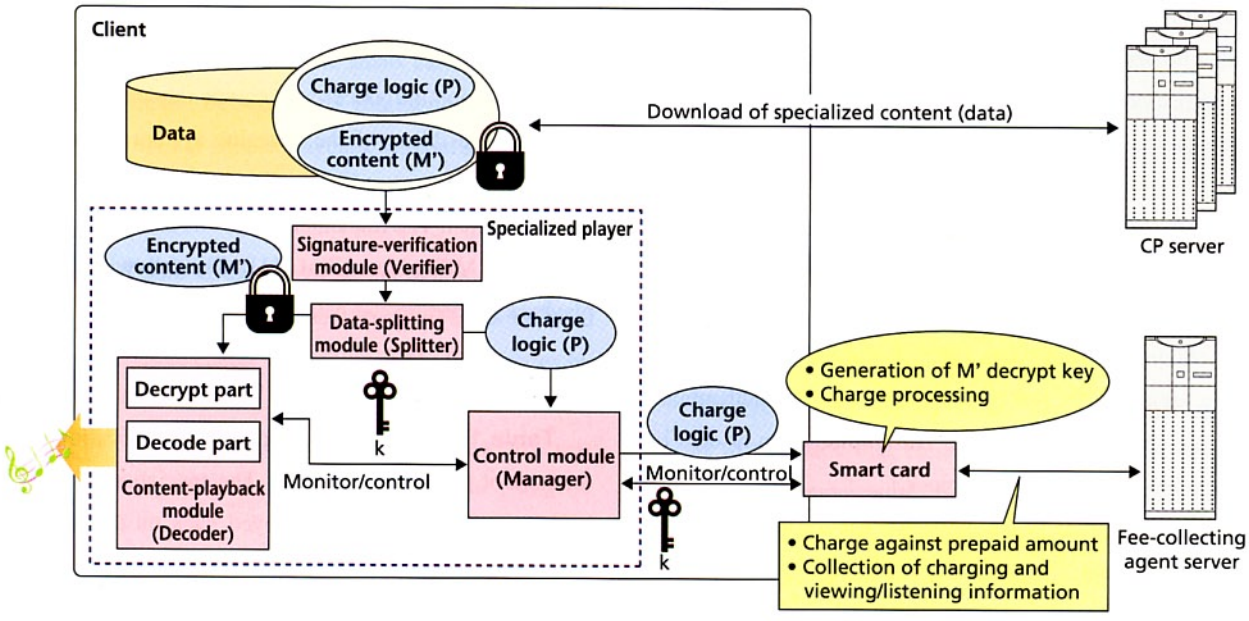

Figure 2 Detailed configuration of specialized player

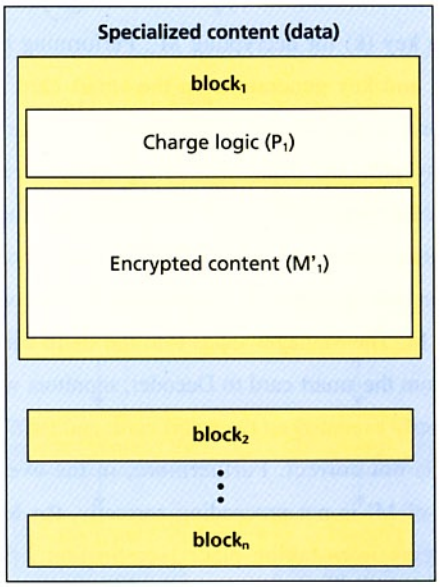

Figure 3 Format of specialized content data

if the amount charged for that content exceeds 300 yen, and to charge nothing after the amount exceeds 700 yen. This information would be written in a special format.

In the implementation reported here, we targeted music data in MP3 (Moving Picture Experts Group-1 Audio Layer-3) format, and considered the following requirements for configuring specialized content (data) using MP3 format.

- The data must take on the same format as an MP3 file.
- Music so configured must not be capable of playback on a general MP3 player.
- Music content must be encrypted.
- Each item of content must be given a digital signature to be checked whether the content has come from a legitimate CP.
- It must be possible to set charge logic for each item of content corresponding to a charge unit and to check whether the charge-amount frame has been correctly decrypted.

To satisfy these requirements, we created data according to the following procedure.

1) Encyrpt a charge-unit's worth of MP3 frame data using key ki to obtain encrypted data (M_i'). Combine this data with charge logic (P_i) for that data plus the message authentication code (MAC_i) of data (M_i). This combination of data is taken to be one block of data ($block_i$).
2) Store the above data in the main data section of audio data in the MP3 format.
3) Store the digital signature assigned by the CP in the header section (ID3v2 tag).
4) Include in the content secret information to be shared by the CP and smart card and encrypted by the specialized player's public key.

2.6 Playback Procedure at the Specialized Player

Figure 4 shows the playback procedure between the specialized player and smart card in detail.

1) The smart card performs user authentication based on a Personal Identification Number (PIN), and the specialized player and smart card exchange the session key (k).
2) The specialized player uses k to encrypt P_i, the decrypt key (k_{i-1}) of the previous charge unit, and the hash value[*2] ($hash_{i-1}$) of content data after decrypting, and sends the result as a charge request to the smart card.
3) The smart card performs charge processing and generates decrypt key k_i, encrypts this decrypt key using k, and sends the result to the specialized player. Here, the generation of decrypt key k_i is performed using k_{i-1} and $hash_{i-1}$.
4) The specialized player decrypts the content data and verifys MAC_i included in $block_i$ of data. If the verification succeeds, it sends a charge-commit request to the smart card and plays back the music. If the verification fails, it sends a charge-rollback request to the smart card and terminates playback.
5) On receiving a charge-commit request, the smart card subtracts a usage fee corresponding to the amount of playback from the prepaid balance. On receiving a charge-rollback request, it performs no subtraction of that fee and terminates processing.

3. Implementation and Evaluation

This section introduces a prototype implementation for verifying the feasibility of the charging system described above. The target content used in this implementation was music data in MP3 format. The implementation was achieved by modifying an existing MP3 player (Zinf [11]). The following describes the playback procedure and data configuration.

3.1 Implementation Results

Table 1 and **Figure 5** describe the specifications and environment of this implementation. The specialized content downloaded via the network was played back on the client PC and the performance of this playback was measured and evaluated.

*2 A hash value is output from a one-way hash function that generates a fixed-length output value from input of arbitrary length. It can be used to check whether data has been altered during transmission.

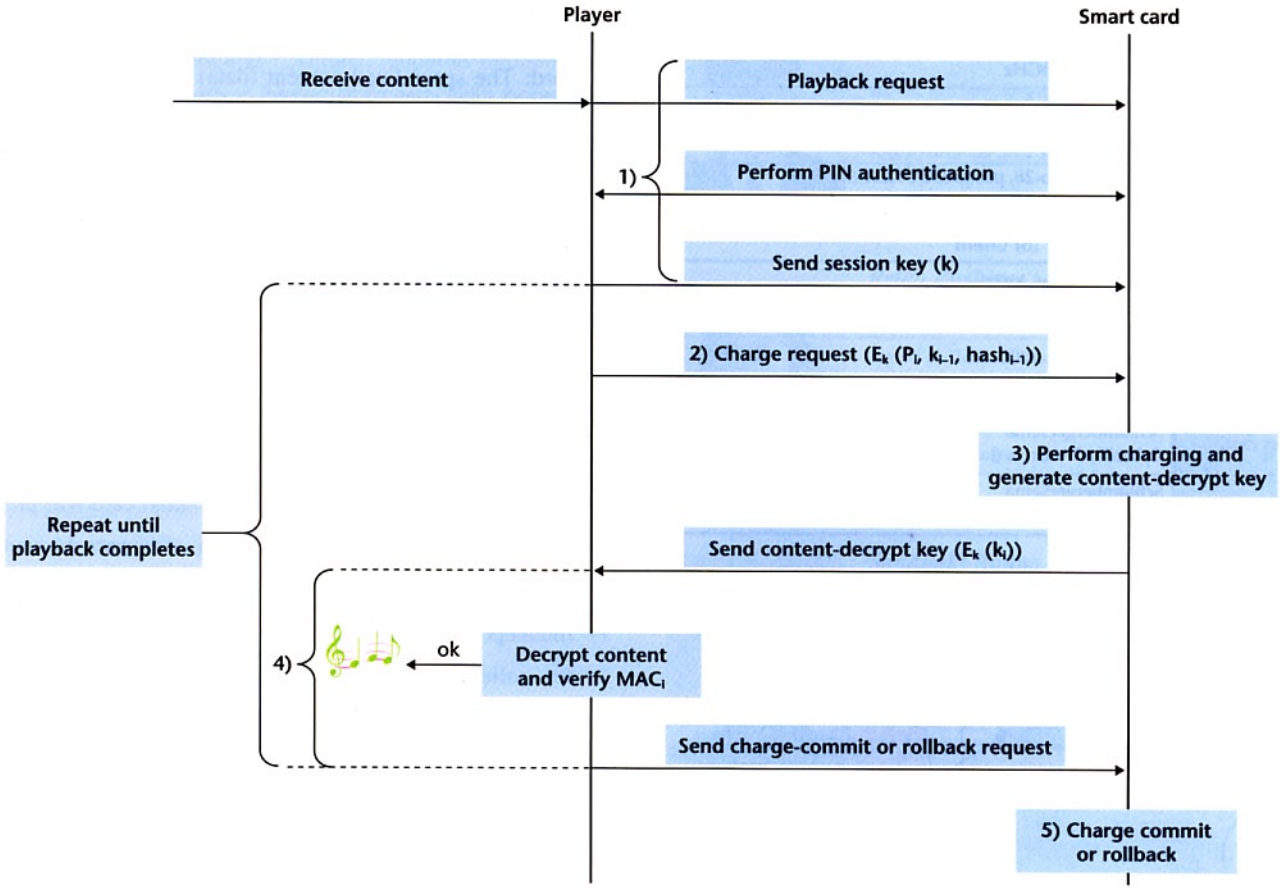

Figure 4 Playback procedure between specialized player and smart card

Compared to ordinary playback, communications with the smart card and processing within the smart card constitute overhead in this implementation, and to prevent skipping, charge-unit time must be set with this overhead in mind. The time taken up by communications with the smart card and by charge processing and key generation within the smart card is about two seconds. It can therefore be seen that a charge-unit time of two seconds or greater should enable playback without skipping and that correct playback can be achieved for charging at two-second intervals.

As shown by **Table 2**, the size of specialized content (data) increases as charge-unit time becomes shorter. This is because the number of entries of charge logic (P) and MAC increases by the number of additional charge units. For a five-minute piece, for example, this increase could come to 150 entries of P and MAC (corresponding to an increase in data size of about 64 Byte × 150).

In the proposed model, content does not necessarily have to be downloaded from the network, which means that increase in data size may not be a serious problem. Nevertheless, if data sizes come to fill up terminal memory or recording media (such as an SD card or memory stick), users may demand smaller data sizes. In such a situation, charge-unit time must be decided taking both this need and security into account.

3.2 Countermeasures to Attack Scenarios

Countermeasures to the attack scenarios described in Section 2.3 with regard to this implementation are discussed below.

1) Overwrite P to prevent correct charging: The CP's signature is included in data and checked by the signature-verification module thereby preventing P included in data from being altered.
2) Observe illegally and record the key for decrypting M' into M to playback that content (extract M from downloaded data): Communications between the specialized player and smart card are encrypted by the session key thereby preventing a decoding key from being leaked.
3) Save analog data generated at playback of M and redistribute that content: An attack related to analog data is outside

Table 1 Implementation environment (basic specifications)

(a) CP server, fee-collecting agent server

CPU	Pentium® 4 2.8GHz
Memory	2GB
OS	RedHat® Linux® 7.3
Other	Openss l0.9.6b-28, postgreSQL 7.2.1-5, Apache™ 1.3.23-14, tomcat 3.3.3.1-4

(b) Client

CPU	Pentium® 3 866 MHz
Memory	512 MB
OS	Windows® XP, 2000
Player	Zinf modified
Smart card	SchlumbergerSema CyberFlex™Access (JavaCard™ 2.1)
Smart card R/W	SchlumbergerSema Reflex20 (PC card)

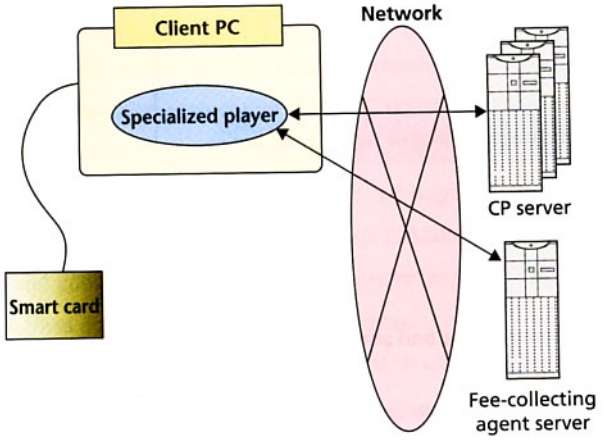

Figure 5 Implementation environment

Table 2 Charge-unit time and increase in data size

Charge-unit Time (sec)	Increase in Data Size (%)
1	17.70
2	13.79
3	12.92
4	12.75
5	12.31
6	11.96
7	11.73
8	11.80
9	11.66
10	11.52

the scope of this study.

4) Directly access the smart card without executing data to alter prepaid money or charge information: Because of the playback procedure in the control module, charge processing does not complete as long as music data cannot be correctly decoded. The tamper resistance of the smart card, moreover, is assumed to be reliable, which means that data inside the smart card cannot be overwritten.

5) Execute data without outputting correct results to the smart card: The specialized content (data) prevents charge logic from being altered. In addition, the end user is required to input a PIN code to access the smart card at the time of content playback thereby making it difficult for someone other than the authorized user to access the smart card.

6) Playback content but falsify output to the smart card at a point between the specialized player and smart card to prevent charge processing from being performed within the smart card: Processing within the smart card is not limited to charging but also consists of key k_i generation. As a result, any alteration of output to the smart card will prevent correct decrypting thereby offering resistance to such an attack.

7) Intercept and falsify interaction between the smart card and fee-collecting-agent server: This attack is dealt with by Secure Sockets Layer (SSL) server authentication. The end user's ID and password are authenticated when charging against the prepaid amount.

4. Conclusion

In this article, we proposed a content charging system that performs charge computation in a manner inseparable from content playback. This system aims to enable unrestrained distribution of content by providing client-side charge processing as opposed to making payment to each content provider by its charging system for each item of content. We also reported on a prototype implementation for testing this system. With this implementation, it was found that charge computation could be executed inseparably from content playback and that playback and charging could be performed appropriately.

We assumed that the specialized player was achieved by tamper-resistant software. In future research, we plan to investigate a system that presumes tamper resistance not just for the specialized player but for an entire system through cooperative interaction between smart cards, specialized players, servers, etc.

REFERENCES

[1] Microsoft Product Activation: http://www.Microsoft.com/japan/windowsxp/pro/techinfo/productactivation/asp

[2] M. Inamura, T. Tanaka and K. Nakao: "Realizing Illegal Copy Protection for Digital Contents," Symposium on Cryptography and Information Security (SCIS), 2003. (In Japanese)

[3] Inamura and T. Tanaka: "Implementation and Evaluation of Illegal Copy Protection for Digital Contents," CSEC-22, Jul. 7, 2003. (In Japanese)
[4] R. Mori, M. Kawahara and Y. Ohtaki: "Superdistribution: The Microelectronic Approach to Intellectual Property Right Processing," Information Processing, Vol. 37, No. 2, 1996. (In Japanese)
[5] K. Kanno: "Operation Management System and Operation Management Method," Patent 1998-83298 (Japan), 1998. (In Japanese)
[6] H. Takata: "Information Management Equipment, Information Management System, and Media for Storing Information Management Software," Patent 2001-249730 (Japan), 2001. (In Japanese)
[7] Keitaide-Music Consortium: http://www.keitaide-music.org/index_j.html
[8] R. Hoshino et al: "The secure charging model on the client, and its application," JIPS 65th National Convention, 2003. (In Japanese)
[9] H. Aono et al: "An Implementation of the Charging system on the client by inseparable processing of content replay and charging," 21st CSEC Group Meeting, 2003. (In Japanese)
[10] H. Aono et al: "Evaluation of the Charging system on the client by inseparable processing of content replay and charging," CSS2003, 2003. (In Japanese)
[11] Zinf: http://www.zinf.org

ABBREVIATIONS

ADSL: Asymmetric Digital Subscriber Line
CP: Contents Provider
CPRM: Content Protection for Recordable Media
CPU: Central Processing Unit
MAC: Message Authentication Code
MP3: Moving Picture Experts Group-1 Audio Layer-3
PIN: Personal Identification Number
SSL: Secure Sockets Layer