N-times Consumable Digital Ticket and
Its Application to Content Access Service

Hyoungshick Kim

Home S/W Platform Team, Software Laboratory
Samsung Electronics
416, Maetan-3Dong, Yeongtong-Gu, Suwon-City, Gyeonggi-Do, Korea 443-742
Hyungsik.kim@samsung.com

Abstract—**In this paper we present a new type of the digital ticket called *N*-times consumable digital ticket for e-commerce. A digital ticket is a certificate that guarantees certain rights of the ticket owner. It can be used for software licenses, resource access, discount coupons, and DRM applications. Depending on the application, consumptions of the ticket can be finitely limited. This type of digital ticket is referred to as *N*-times consumable digital ticket. For protecting the consumer's privacy, the *N*-times consumable digital ticket has the similar properties to electronic cash. However, the *N*-times consumable digital ticket can secure the owner's privacy to a higher level compared with electronic cash since the *N*-times consumable digital ticket protocol can conceal not only the owner's identification but also the quantity of the ticket consumed. We propose the protocol for secure *N*-times consumable ticket issuing over the Internet by using cryptographic primitives such as blind signature and hash chain. We also demonstrate its utility by showing its application to content access service for guaranteeing a customer's privacy.**

Keywords-component; Digital ticket, Cryptographic protocol, Anonimity, Privacy, Content Access Service

I. INTRODUCTION

These days, the Internet enables people to efficiently collect and process useful information and to acquire diverse goods and services online without physical contact. Thus, various electronic payment schemes such as encrypted credit cards, electronic cash, and a micropayment system have been designed and implemented for e-commerce [1][2][3][6]. However, in the opposite flow of the payment, goods or products to the consumer is dependent on a physical delivery system except for a few types of digital content such as images, audio, video, and software programs [5].

Digital tickets appear to be a useful solution for types of service such as transportation, accommodation, theater, gift certificate, coupon, stamp and digital contract, since service rights can be sold as digital tickets via the network [4][11][18][19]. A digital ticket is a certificate which guarantees that the ticket owner has the rights to claim the services written on the ticket. The ticket may be delivered and stored electronically [7]. After the completion of purchasing goods or services online, a service provider on a network issues a digital ticket (or a digital credential) instead of the physical delivery of them [4][19]. Therefore a consumer receives the

digital tickets and records them to allow access the service or exchange of goods later.

In general, the fundamental digital tickets can be used only once, i.e., the digital ticket should be invalidated after the service has been provided. On the other hand, there are also digital tickets which can be used more than once. We call such a digital ticket as *N*-times consumable digital ticket. In this paper, we are particularly interested in this type of digital ticket. Offering such digital tickets can be beneficial for both service provider and consumer since the consumer is bound to the specific service provider. When the provider issues the ticket, the consumer can conveniently maintain his rights to the service in a long term transaction such as a subscription service.

The concept of e-commerce using the digital tickets has been previously implemented in many practical applications. For example, 'e-gold' or gift certificates in 'Apple iTunes' have already been developed and commercialized [8][20]. Brands introduced the concept of the digital ticket in 1993 [16]. The work of Fujimura et al. and Stefik proposed a system for controlling the distribution and use of digital works using digital tickets [5][10]. Susanne et al. mainly focused on managing the digital contract between different players [11]. However, conventional digital tickets or similar approaches enable ticket issuers or service providers to easily monitor and record a consumer's behavior during the issuing and consuming of the ticket, which may cause a problem in that the sensitive information of the consumer is revealed. Such consumer information might be exploited for data mining, to infer new consumer data, consumer profiling, promotion of new products, price discrimination, etc. [12][13][19].

In this paper, we propose a protocol for e-commerce using a *N*-times consumable digital ticket, by which privacy is guaranteed so that information of a digital ticket consumer is exposed minimally and the use of a service is facilitated. This scheme enables the ticket consumers to use his/her tickets without revealing the sensitive information of him/her like the value written on the ticket.

The remainder of the paper is structured as follows: In section 2, we present the model of a *N*-times consumable digital ticket. In section 3, we describe the proposed scheme in detail. In section 4, we then demonstrate the utility of the
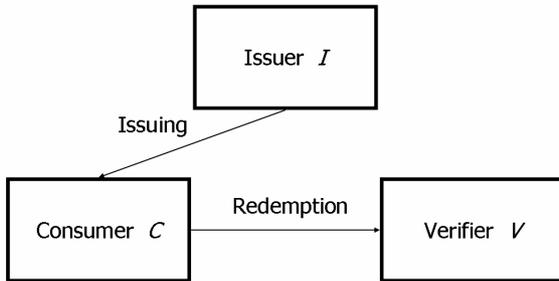
proposed protocol by introducing a content access application. Finally, we conclude the paper and give an overview of future activities in section 5.

II. MODEL

In this paper, N-times consumable digital ticket system is defined as follows [5][15].

A. Players

The players of a N-times consumable digital ticket system are shown in Figure 1.

Figure 1: Generic Model of a Digital Ticket System

The digital ticket is generated by a ticket issuer, denoted I. The ticket issuer I has business relations with certain service providers who act as ticket verifier providing the demanded online goods.

The generated digital ticket is unique. In most current systems, a unique random number is included in the digital ticket. Under the agreement with the ticket consumer, I issues the N-times consumable digital ticket to the consumer.

A ticket consumer (or a service consumer), denoted C, receives a N-times consumable digital ticket from I. In general, it is required that the received ticket should be securely stored by C (or the device of C). The best device would be a secure isolated device like a tamper-resistant smartcard that can be always connected to I and online merchants via computer or hand-held device [14]. When C receives the ticket, its validity should be checked. If the ticket has something wrong, C rejects the request and asks I to reissue the digital ticket.

Denote V a ticket verifier who is under contract to I. V verifies the validity of the digital ticket. Then, V provides the service or goods designated on the digital ticket C. A ticket is valid if it has been issued by a legal ticket issuer and has not been used by this time.

In this paper, we assume that since I and V are physically deployed together in most practical applications, they are the same player without loss of generality [19].

B. Requirements

In this section, we consider a range of potential requirements for each player involved in the digital ticket consumption process: a ticket issuer/verifier I ($= V$) and a ticket consumer C.

1) Issuer/Verifier Requirements

- **Unforgeability.** A legal issuer I can only generate the ticket and issue it.

- **Detection duplication.** Double-consuming or duplication of a digital ticket should be either prevented or detected.

- **Prevention of revision.** Given N-times consumable digital ticket, it must be infeasible to increase the number of consumable times.

2) Consumer Requirements

- **Anonymity.** Given a N-times consumable digital ticket, it must be infeasible to guess the consumer's identity.

- **Secrecy of the times.** Given a N-times consumable digital ticket, it must be infeasible to guess the number of remaining consumable times of the ticket.

It is important that a digital ticket should disclose as little information as possible, i.e., in the step of 'Redemption' only the validity of the ticket should be revealed since the sensitive information such as the remaining consumable times hints at the identity of the ticket consumer [19].

III. OUR PROTOCOLS

In this section we propose a system that allows issuance and redemption of a N-times consumable digital ticket by using some cryptographic primitives. The system is comprised of the 'Issuing' protocol and the 'Redemption' protocol which are both carried out between I and C.

A. The cryptographic primitives

Our proposed system has the following cryptographic primitives.

1) Blind signature

In 1982, the concept of the blind signature was introduced by Chaum for untraceable electronic cash [21]. A blind signature scheme is an interactive protocol that involves two-parties, a signer and a user. The scheme allows the user to obtain the signed message in a way that prevents the signer obtaining any other information about the content or the sender of the message. Several signature schemes have been turned into blind signature schemes.

A blind signature scheme BS is defined as a 5-tuple of algorithms (G, S, V, B, U) such that G, S, V have the same characteristics of a conventional digital signature scheme and B, U are as follows:

- The Blinding algorithm B is a probabilistic polynomial-time algorithm with a blind key b and a message m. The algorithm also produces output $b(m)$ which we call the blinded message of m.

- The Unblinding algorithm U is a probabilistic polynomial-time algorithm with a blind key b and a signed message $SIG_k\{ b(m)\}$. The algorithm also produces output $SIG_k\{m\}$ which means that m is signed by the sign key k.

Without the blind key b, it is unlikely to obtain the meaningful information from the blinded message $b(m)$.

2) Hash Chain

One-way hash chain is a frequently used cryptographic primitive in the design of secure protocols. Given a one-way hash function H, for setup of one-way chain ($V_0 \ldots V_N$), the generator selects the initial value V_N at random, and iteratively applies the one-way hash function H, i.e., the generator computes that $V_i = H(V_{i+1})$, for $0 \le i < N$. An example of a standard hash chain is shown in Figure 2 [17].
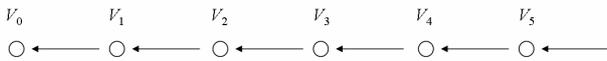
Figure 2: Standard one-way hash chain

If we assume H is cryptographically secure one-way function, a hash chain of H provides the following two properties.

- Given only a value V_i of the chain, it is intractable to compute a value, where $j > i$, such that $H^{j-i}(V_j) = V_i$.

- Given two values V_j and V_i, it is easy to check that $H^{j-i}(V_j) = V_i$, where $j > i$.

The security of the one-way hash chain is based on the selection of the cryptographic one-way hash function such as SHA-1, $MD5$, and pseudo-random functions (PRF) [9][22][23].

In our protocol, we choose a pseudo-random permutation (PRP) (e.g., a block cipher) which is a one of the PRF family as the basic one-way hash function since PRP provides the property that the length of $H(V_i)$ is the same as the length of V_i.

B. Construction of the digital ticket system

For the construction of the ticket system, it is needed to share some information between I and C.

A customer C has a unique identity, denoted by ID_C. Without loss of generality, we assume that $|ID_C| = m$ bits.

Let H be the cryptographically secure one-way hash function shared between two players where H is a pseudo-random permutation of l bits to l bits and $m < l$.

Also I and C must agree to use some secure blind signature scheme $BS = (G, S, V, B, U)$. In the first step, I runs the key generation algorithm G in BS to generates a pair of keys (pk, sk). The key generation algorithm G is locally run by I. The issuer I will issue the valid ticket using sk, and others including I will verify the validity of the signed ticket using pk which I has issued. In the second step, I registers pk to some trusted server which acts like a public phone book. Someone wishing to obtain pk can request it from the server by sending the identity of I and returning pk. After the obtaining pk, C uses pk and, in addition, C freely chooses the blind key b in the blinding algorithm B.

In addition, I chooses some random permutation p which is of m bits to m bits where ID_C is an element of the domain of p. The one-way property of p is unnecessary, but the selected p must at least satisfy the property of the randomness. After selecting p, the ticket issuer I should publish the selected p in the similar to the public key pk.

The proposed system consists of two protocols, 'Issuing' and 'Redemption' which are carried out between an issuer I and a consumer C.

Before the 'Issuing' step, C enters into a contract with I in order to assign the ownership of a N-times consumable digital ticket to C. The interesting feature is that the consumer C triggers the protocol before the issuer I to protect his/her privacy. If I runs the 'Issuing' step by him/herself, the anonymity of C cannot be preserved as I can always link the identity of C in the 'Issuing' step with the uniqueness of the issued ticket. For preventing the duplication of the digital ticket, I should uniquely generate the ticket. To invade C's privacy, I records the unique information of the ticket, the identity of C and the relation between them in a large database. In the step of 'Redemption', I can infer the identity of C by using the recorded information in the database when C requests to consume the digital ticket.

1) Issuing

In the 'Issuing' step, C firstly accesses the published random permutation p.

By using p, C computes s as follows:

$$s = p(ID_C) \tag{1}$$

In order to prevent the customer's cheating, the "cut and choose" procedure will be used, i.e., C should choose k random numbers of (l - m) bits which is given a security parameter 1^k as follows:

$$r_1, r_2, \ldots, r_k \tag{2}$$

From (1) and (2), C computes k initial tickets $T_{i, 0}$ as (3). $\|$ denotes the string concatenation.

$$T_{i, 0} = H(s \| r_i), \text{ for } 0 \le i < k \tag{3}$$

After computing k initial tickets $T_{i, 0}$, C then sequentially computes $T_{i, j}$ by repeatedly applying the one-way hash function, for $0 \le j \le N$, as follows:

$$T_{i,j+1} = H(T_{i,j}), \text{ for } 0 \le i < k \text{ and } 0 \le j \le N \tag{4}$$

After computing the end tickets in all hash chains, C should keep k initial tickets $T_{i, 0}$ and k end tickets $T_{i, N+1}$ in secure storage such as on a tamper resistant smartcard device

to prevent loss or modification. To increase efficiency, C can also keep the all intermediately computed values depending on the application.

Finally, C generates k blinded tickets using k blind keys b_1, b_2, … , b_k as follows:

$$B_i = b_i(T_{i, N+1}), \text{ for } 0 \le i < k \qquad (5)$$

C then sends the k blinded tickets B_1, B_2, … , B_k, generated in (5) to the issuer I. At this time, I cannot believe that all k received messages are honestly generated by C, through the correct procedure from (1) to (5), since all received messages are the blinded using b_1, b_2, … , b_k. which C has chosen.

By using "cut and choose" procedure, I can prevent or detect the cheating of C, i.e., C must comply with the correct procedure.

In the first step, I selects the one of the k blinded tickets at random, and requires that C unblinds all of the rest except the randomly selected blinded ticket. We assume that the selected index is x.

In the second step, C must deliver all blind keys b_1, b_2, … , b_k. and the random numbers r_1, r_2, … , r_k in (2) except b_x and r_x as requested by I. Before issuing the tickets, I checks that all of the unblinded $T_{i, N+1}$ are correct except $T_{x, N+1}$. I can check them in the similar manner, (1) to (5), using all the received blind keys and random numbers. However, I still has no information about $T_{x, N+1}$ since I cannot open B_x without b_x.

In the third step, I signs B_x using sk and then issues it to C, if all of the unblinded $T_{i, N+1}$ are correct.

Finally, when C receives the signed B_x, he/she checks the validity of I's signature using pk. If it is valid, C computes the N-times consumable digital ticket $\{T_{x, N+1}\}_{sk}$ using the unblinding algorithm U and the private blind key b_x in BS as the follows.

$$\{T_{x, N+1}\}_{sk} = U(\{b_x(T_{x, N+1})\}_{sk}, b_x) \qquad (6)$$

C securely stores $\{T_{x, N+1}\}_{sk}$ calculated in (6), together with r_x.

2) Redemption
C computes $T_{x, N}$ using r_x in a similar manner, (1) to (4), and then sends the stored $\{T_{x, N+1}\}_{sk}$ and $T_{x, N}$ to I.

In the 'Redemption' step, I checks four points for the validity of the received ticket.

I checks the signature of $\{T_{x, N+1}\}_{sk}$ and if it is valid, computes the following equation.

$$T_{x, N+1} = H(T_{x, N}) \qquad (7)$$

If (7) is valid, I must check whether $T_{x, N}$ is the pre-image of the initial ticket as (8). $pre_k(s)$ denotes the prefix of the k bits of the string s.

$$p(ID_C) = pre_m(T_{x, N}) \qquad (8)$$

If the equation of (8) is true, I rejects the ticket since it means that the remaining consumable number of times of the digital ticket is 0. Otherwise, I must check the duplication of the ticket $\{T_{x, N+1}\}_{sk}$. For detection of duplicated tickets, I records all of the previously consumed tickets in a large database. By using the database, I can check in real time whether the received ticket was already consumed, i.e., I can search for the same value as $T_{x, N+1}$ in the database.

If this is the first time the ticket $\{T_{x, N+1}\}_{sk}$ is being consumed then, I accepts it. Otherwise, he/she rejects it. In the case of acceptance, I provides the service or the good and then send the newly signed $\{T_{x, N}\}_{sk}$ to C. Also, I records $T_{x, N+1}$ in the database to avoid the duplication of the already consumed ticket in the future.

C. Security of N-times consumable digital ticket
Most requirements are directly satisfied by the blind signature and cryptographically secure one-way hash chain.

For unforgeability, it is clear that it is impossible to forge the digital ticket if I and C agree the adoption of a cryptographically secure blind signature scheme.

For detection of duplication, we show that I can detect the previously consumed tickets by using a database.

For prevention of revision, C may cheat I on the consumable times of the ticket in the issuing step since I requests to unblind the only k-1 blinded B_1, B_2, … , B_k except B_x. i.e., C can cheat I if I does not require to unblind the fabricated ticket in "cut and choose" procedure. However it is sufficiently small possibilities for cheating (exactly k^{-1}).

For maintenance of anonymity, security of the overall system is based on the infeasibility of the blinding algorithm B in the blind signature scheme BS. To protect C's privacy, C does not reveal the pre-image of the initial ticket in a hash chain since I can get ID_C from it. Therefore C can consume the digital ticket exactly N times.

In maintaining secrecy of the times, it is clear that I cannot guess the remaining consumable times of the ticket since a pseudo random permutation is used as one-way function H in our proposed system.

IV. CONTENTS ACCESS APPLICATION

In practice, the N-times consumable digital ticket system can be directly mapped to a content access application. We have a triple of players: O, C and S. A gift ticket office O, a content access client C, and a content access service S are implemented as a web service, as the software on a PC, and as a web service respectively.

In the scenario of downloading N items of content onto a user's PC, a gift ticket can be used to preserve his/her anonymity. Without requesting a login to the service S, a gift ticket enables user to privately download the contents provided by S if S provides content in exchange for ticket consumption.

At the system level, it is important that the client software *C* must not be provided as closed solution by *O*. To guarantee the privacy of user, the client *C* is needed to be transparently open and fair software as much as possible.

V. CONCLUSION

We have presented a system for e-commerce using *N*-times consumable digital ticket based on cryptographic primitives such as the blind signature and the one-way hash chain.

To protect the privacy of consumers, the *N*-times consumable digital ticket system conceals not only the identity information of the consumer but also the remaining consumable times in the ticket. We proposed a simple and secure ticket system.

In practice, our proposed system can be used for many applications such as software licenses, discount coupons, and DRM applications. We have demonstrated that the proposed system can be directly mapped to contents access applications.

In the future, we plan to investigate how our system can be extended to support the unlinkability between the generated tickets and transferability of a ticket among consumers. We will also investigate a formal security proof of the system.

REFERENCES

[1] N. Asokan, P. A. Janson, M. Steiner, and M. Waidner, "The State of the Art in Electronic Payment Systems," IEEE Computer, Sep. 1997, pp. 28-35.

[2] M.E. Peter, "Emerging ecommerce credit and debit card protocols," Electronic Commerce, Oct. 2002, pp. 39-46.

[3] I. Papaefstathiou, C. Manifavas, "Evaluation of Micropayment Transaction Cost", Journal of Electronic Commerce Research, Vol. 5, No. 2, 2004, pp. 99-114.

[4] S. Brands, "A technical Overview of Digital Credentials," Research Report, Feb. 2002.

[5] K. Fujimura and Y. Nakajima, "General-Purpose Digital Ticket Framework," the 3rd USENIX Workshop on Electronic Commerce, Sep. 1998.

[6] P. Wayner, Digital Cash, Academic Press Ltd., 1997.

[7] M. Terada, H. Kuno, M. Hanadate, and K. Fujimura, "Copy Prevention Scheme for Right Trading Infrastructure," the 4th Smart Card Research and Advanced Application Conference, Sep. 2000.

[8] Gold & Silver Reserve, Inc., "e-gold," http://ww-w.e-gold.com/

[9] O. Goldreich, S. Goldwasser, and S. Micali, "How to construct Randomfunctions," Journal of the ACM, 33(4):792-807, Oct. 1986.

[10] M. Stefik, "Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing," Berkeley Technology Law Journal Vol. 12. No.1, 1997, pp. 137-159.

[11] S. Guth, G. Neumann, and M. Strembeck, "Toward a Conceptual Framework for Digital Contract Composition and Fulfillment," In Proc. of the International Workshop for Technology, Economy, Social and Legal Aspects of Virtual Goods, May 2003.

[12] S. G. Stubblebine and P. F. Syverson, "Authentic Attributes with Fine-Grained Anonymity Protection," Financial Cryptography, 2000.

[13] A. Odlyzko, "Privacy, Economics, and Price Discrimination on the Internet," 5th International Conference on Electronic Commerce, 2003.

[14] M. Terada, H. Kuno, M. Hanadate, and K. Fujimura, "Copy Prevention Scheme for Rights Trading Infrastructure," 4th Smart Card Research and Advanced Application Conference, Sep. 2000.

[15] K. Fujimura, M. Terada, and J. Sekine, "A World Wide Supermarket Scheme Using Rights Trading System," The International Workshop on Next Generation Internet Technologies and Application, Jul. 2000.

[16] S. Brands, "Privacy-protected transfer of electronic information." U.S. Patent No. 5,604,805, Feb. 1997.

[17] Y. Hu, M. Jakobsson, and A. Perrig, "Efficient Constructions for One-Way Hash Chains," TR CMU-CS-03-220, Nov. 2003.

[18] R. Pear, "Electronic cards replace coupons for food stamps," New York Times, Jun. 23, 2004.

[19] L. Chen, M. Enzmann, A. Sadeghi, M. Schneider, and M. Steiner, "A Privacy-Protecting Coupon System. Financial Cryptography," 2005, pp. 93-108.

[20] A. Wibowo, K. Lam, G. Tan, "Loyalty program scheme for anonymous payment systems," Electronic Commerce and Web Technologies, LNCS 1875. Springer, 2000.

[21] D. Chaum, "Blind Signatures for Untraceable Payments.Proceedings," Crypto, 1982.

[22] National Institute of Standards and Technology (NIST), "Secure hash standard," May 1993. Federal Information Processing Standards Publication 180-1.

[23] R. L. Rivest, "The MD5 message-digest algorithm," Internet Request for Comment RFC 1321, Internet Engineering Task Force, Apr. 1992.