COPY PREVENTION SCHEME FOR RIGHTS TRADING INFRASTRUCTURE

Masayuki Terada
NTT Laboratories
te@isl.ntt.co.jp

Hiroshi Kuno
NTT West
kuno.hiroshi@nagoya.west.ntt.co.jp

Masayuki Hanadate
NTT Laboratories
hanadate@isl.ntt.co.jp

Ko Fujimura
NTT Laboratories
fujimura@isl.ntt.co.jp

Abstract This paper proposes FlexToken, a new copy prevention scheme for digital rights such as tickets or coupons, which are circulated as pieces of paper in the real world. The important feature of this scheme is that digital rights are represented using two separate types of information: the contents and the token of the rights. The token represents the "genuineness" of the contents and distinguishes the genuine digital rights from copies. A token is stored and circulated using tamper-proof devices such as smartcards while the contents can be held in any storage medium. This approach decreases the amount of memory required of the tamper-proof devices. Furthermore, circulating the identity of the right issuer and accredited information, which specifies the tamper-proof devices trusted by the issuer, along with a token makes it possible to protect any type of digital right, regardless of the issuer.

Keywords: Electronic commerce, smartcard, copy prevention, rights trading, ticket, coupon.

1. INTRODUCTION

Rights are traditionally circulated as pieces of paper such as tickets and coupons. By circulating rights as digital data (digital rights) instead of pieces of printed paper, tickets can be sold over the Internet and the cost for issuing and collecting tickets can be decreased[Fujimura, 2000] [Xerox Corporation, 1998].

Unlike paper tickets, however, it is difficult to discern "genuine" digital data from copies. For digital rights to be circulated in the same way as tickets, a mechanism must be implemented that either detects copies or prevents copying of such data.

A copy prevention scheme for digital rights must meet the following requirements:

1 It must handle various types of rights issued by different issuers.

2 It must prevent illegal acts such as forgery and reproduction, and guarantee security such as ensuring privacy.

3 It must be practical to implement in terms of efficiency and convenience.

Each of these requirements is discussed below in detail.

- Handling diversity

  Various types of rights Unlike an electronic cash system that only deals with a specific currency, the system must prevent copies of various types of rights, from securities and checks to concert tickets.

  Different issuers Unlike an electronic cash system that only deals with a currency issued by a specific issuer such as a central bank, the system must handle digital rights issued by different issuers.

- Ensuring security

  Preventing alteration Digital rights must not be altered during circulation.

  Preventing forgery Digital rights must not be counterfeited. Only the issuer may make duplicates.

  Preventing reproduction Digital rights must not be reproduced while in circulation.

  Ensuring fairness It should not be possible to repudiate the transfer of rights when they are handed over or sold.

Ensuring privacy Current and previous ownership of rights should be concealed.

- Ensuring practicality

  Scalability It should be possible to handle a large number of rights. A centralized server, which tends to be overloaded by the concentration of requests, should be avoided.

  Off-line capability It should be possible to circulate digital rights without using a network.

  Cost efficiency It should be possible to issue and use rights at a reasonably low cost and without depending on expensive devices.

This paper proposes a copy prevention scheme called FlexToken that satisfies the above requirements. This scheme uses taper-proof devices such as smartcards for basis of security. Since this approach does not depend on centralized servers, it is possible to ensure scalability and off-line capability.

This scheme divides the digital right to a definition of the right and the genuineness of the right. The former is treated as usual digital information while the latter is handled by smartcards in order to block illegal acts as mentioned above. The division of the right enables the scheme to handle diverse types of digital rights using quite realistic smartcards which are not so expensive.

Furthermore, the proposed scheme enables any issuer to circulate rights using the accredited information, which specifies a trust domain of the issuer.

2. OVERVIEW

This section discusses the participants and transactions involved in the digital rights circulation model that we assumes, and explains the basic concepts of our scheme.

2.1. PARTICIPANTS AND TRANSACTIONS

Digital rights are circulated among three types of participants: issuer, user and collector, by three types of transactions: issue, transfer and redeem (Figure 1). Each of the participants and the transactions are defined below.

2.1.1 Participants.

Issuer A participant who issues and underwrites digital rights.

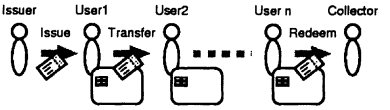

Figure 1 Life cycle of rights

User A participant who transfers and redeems (consumes and presents) the digital rights. It is assumed that each user has his own smartcard.

Collector A participant who collects the digital rights.

2.1.2 Transactions.

Issue transaction An action in which the issuer creates a digital right and gives ownership of the right to the user.

Transfer transaction An action in which the user transfers the ownership of the digital right to another user.

Redemption transaction An action in which the user redeems the digital right to the collector. There are two types of transactions for a redemption transaction, i.e., consumption and presentation. The consumption causes the right to disappear, but the presentation only confirms the user's ownership of the right, which does not disappear. Generally, certain goods or services corresponding to the right may be given to the user by the collector, in the consumption or the presentation transaction.

2.2. BASIC CONCEPTS

An easy approach to implement such digital rights is to apply an electronic cash system such as Mondex[Mondex International,][Clarke, 1996], as it is. Smartcards, such as those used in an electronic cash system, can hold and transfer a value securely by establishing a secure communication path. This value is primarily used as an amount of money, but it can also be used as an amount of a type of rights.

However, this approach requires users to hold a number of smartcards corresponding to types of the rights. Although some electronic cash systems can hold more than one value in order to support different currencies, they handle only a few limited types of rights, those issued by the issuers preselected by the smartcard issuer. Thus, this requires considerable cost and labor to issue and manage the smartcards.

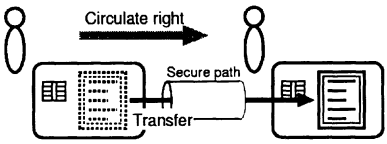

Figure 2 Transfer of a digital right stored in a smartcard

An alternative approach is to transfer the contents of the right instead of just the amount of the right (Figure 2). This approach seems to make it possible to handle all types of rights with a single smartcard, but it is difficult to implement digital rights.

The reasons why the above approach is ineffective include: (1) The capacity of a smartcard may be insufficient because there are various types of rights with different conditions and contents; (2) Although there will be many different issuers of digital rights, smartcards can handle only a limited number of preselected issuers, as in the previous method; and (3) It is impossible to find a smartcard that can be trusted by all issuers because the trust domain may vary depending on the rights issuer[1].

To solve the problems mentioned above, the proposed scheme divides a digital right into two separate pieces of information. One is a rights definition which is stored on a standard storage medium (such as a hard disk) and the other is a token which is stored in a smartcard (Figure 3). The rights definition specifies contents and conditions of the digital right while the token represents the genuineness of the right and guarantees the uniqueness of the right. The token is compact enough (40 bytes in our implementation) to be stored in smartcards and protected against reproduction by them. A token does not represent a digital right by itself but does represent a digital right with a check against corresponding rights definition. A digital right is valid only when the rights definition is verified by the token. A token is equivalent to an irreproducible piece of paper in a conventional ticket, in a sense that both of them represent genuineness.

A token comprises two types of information: one links the token with a rights definition (manifest) and the other identifies the issuer of the digital right (issuer information) (Figure 4). It also employs information called accredited information to be created by an issuer which designates which smartcards the issuer trusts. Thus, it is possible to circulate a digital right using only those smartcards that are trusted by the issuer, and allow anyone to become an issuer of digital rights. Details on how rights are circulated in the proposed scheme are explained in Section 3.

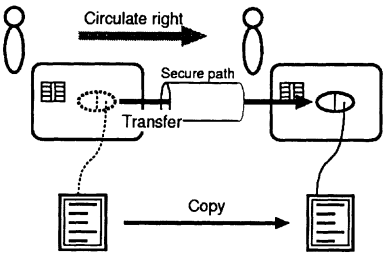

Figure 3 Separation of a digital right

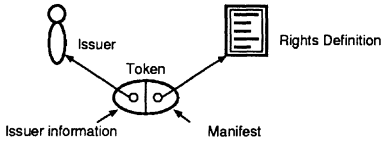

Figure 4 Structure of a token

3. CIRCULATION OF DIGITAL RIGHTS

This section describes the structure of information required to circulate digital rights based on the proposed scheme and circulation procedure.

In this scheme, each participant X has a key pair in public key cryptography: a public key PkX and a secret key SkX. However, the secret key of the user is stored in the user's smartcard and must be concealed from everyone including the user himself. The secret key of the issuer or the collector may be stored anywhere (such as a hard disk), but it must be kept secret from everyone but the owner of the key.

The secret key SkX is used to create a signature in this scheme. In this paper, since a signature to m by SkX is represented as $S_{PkX}(m)$, secret keys are not expressed explicitly. The signature $S_{PkX}(m)$ is verified by verification function $V_{PkX}(\cdot,\cdot)$, which can be composed of the corresponding public key PkX. The verification function has the range as follows:

$$V_{PkX}(m,s) = \begin{cases} true & (s = S_{PkX}(m)) \\ false & (s \neq S_{PkX}(m)) \end{cases}$$

$H(\cdot)$ represents a secure hash function such as SHA-1 or MD5. Similar to SPKI[Ellison et al., 1999], a hash value of the public key in such a function (aka fingerprint), $H(PkX)$, is assumed as an identity of the participant.

3.1. STRUCTURE OF INFORMATION

As explained in Section 2, a digital right consists of a rights definition and a token. The rights definition can be freely copied, but the token must be prevented from duplication or alteration during circulation. Accordingly, some additional information is used in order to achieve this.

The information used to circulate digital rights in FlexToken is structured as described below[2]:

Rights definition This indicates the contents of a right such as the value obtained in and conditions for redemption. Any method, XML Ticket[Fujimura et al., 1999] for example, can be used to describe and interpret the rights definition. Rights definition is represented as m.

Token This is 2-tuple information (t_1, t_2) that represents genuineness of a right. t_1 is a manifest that corresponds to rights definition and t_2 is the issuer information that indicates the issuer of the digital right. Typically, a hash value of rights definition is used as the manifest and the issuer's fingerprint is used as the issuer information. A user who has the token $(H(m), H(PkI))$ in his smartcard is regarded as the holder of the digital right that corresponds to m and I.

Token exchange format (TEF) This is 6-tuple information $(e_1, ..., e_6)$ which is used in transferring a token when circulating a digital right. This information incorporates the sender's signature, which is assigned to the combination of a token and a challenge (described below). Details of TEF are explained in Section 3.2.

Challenge This is 2-tuple information (c_1, c_2) sent from the receiver of a token to the sender when a token is transferred in order to prevent its reproduction by reusing the TEF. c_1 is the fingerprint of the receiver and c_2 is a serial number generated by the receiver.

Tamper-proof guarantee (TPG) This is 2-tuple information (g_1, g_2) which states that the tamper-proof capability of a smartcard is guaranteed by a third party (guarantor). Typically, vendors or issuers of smartcards act as the guarantors. g_1 is a signature to the public key of smartcard by the guarantor and g_2 is the public key of the guarantor. Each smartcard has an appropriate TPG.

Accredited information This is 3-tuple information (a_1, a_2, a_3) which provides the trust domain of an issuer by indicating which smartcard guarantors are trusted by the issuer. a_1 consists of a set of fingerprints of the guarantors of smartcards. The smartcard is considered to be trusted by the issuer, when its TPG is signed by the guarantors included in a_1. a_1 is prevented from alteration by a_2 and a_3. a_2 is a signature by the issuer and a_3 is the issuer's public key.

Receipt This is 2-tuple information (r_1, r_2) which is sent from the receiver to the sender to show that a TEF was accepted. r_1 is the signature to the challenge by the receiver and r_2 is the receiver's public key.

In addition to the above information, each user and collector maintain an issuer list L, a set of fingerprints of issuers. The user and the collector regard digital rights issued by the listed issuers as effective.

3.2. CIRCULATION PROCEDURE

The following sections explain how digital rights are issued, transferred, and redeemed using the above elements.

3.2.1 Issue Transaction. The issue transaction creates a digital right corresponding to rights definition m and transfers the digital right from issuer I to user[3] U. This transaction is performed in the following way (Figure 5):

1 Issuer I creates accredited information $A_I : (a_1, a_2, a_3)$. A_I consists of:

$$\begin{aligned} a_1 &:= \{H(PkG_1), H(PkG_2), ..., H(PkG_n)\} \\ a_2 &:= S_{PkI}(H(PkG_1)||...||H(PkGn)) \\ a_3 &:= PkI \end{aligned}$$

Accredited information A_I is not used in this transaction, but used in transfer and redemption transactions.

2 $I \rightarrow U : \{A_I, m\}$; Issuer I sends A_I to user U together with the rights definition m. The notation $A \rightarrow B : X$ means A sends information X to B.

3 U generates challenge $C_U : (c_1, c_2) := (H(PkU), s)$. s is generated by a incremental serial number generator in U and added to a session database S_U which consists of a set of valid challenges.

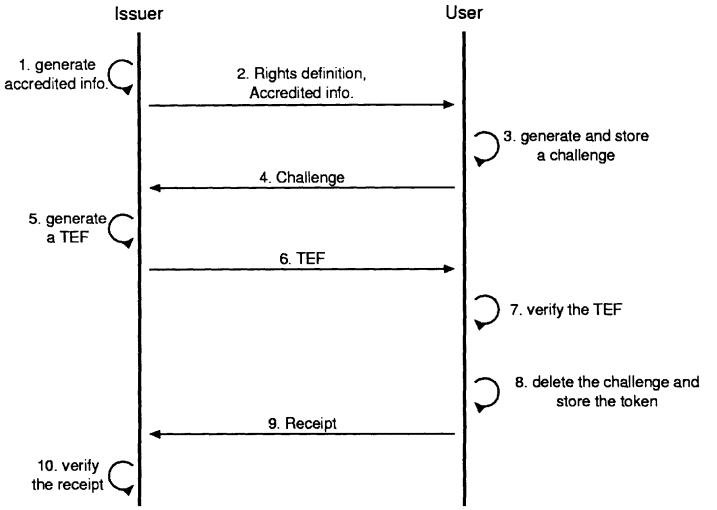

Figure 5 Issuing a digital right

4 $U \rightarrow I : C_U$; U sends challenge C_U to I.

5 I generates a TEF $E_I : (e_1, ..., e_6)$, which consists of:

$$\begin{aligned} e_1 &:= H(m) \\ e_2 &:= H(PkI) \\ e_3 &:= c_1 \\ e_4 &:= c_2 \\ e_5 &:= S_{PkI}(e_1||e_2||e_3||e_4) \\ e_6 &:= PkI \end{aligned}$$

I may have a back-up copy of E_I to respond to unexpected termination of the transaction until a corresponding receipt is sent.

6 $I \rightarrow U : E_I$.

7 U verifies E_I. The verification is successful when the following formulas are satisfied:

$$\begin{aligned} e_3 &= H(PkU) && (1)\\ e_4 &\in S_U && (2)\\ V_{e6}(e_1||e_2||e_3||e_4, e_5) &= true && (3)\\ H(e_6) &= e_2 && (4) \end{aligned}$$

Equations (1) and (2) verify the validity of the challenge. Equation (3) verifies that E_I is surely created by I. Equation (4) verifies that I issued a digital right underwritten by himself.

8 If the verifications above are successful, U deletes e_4 from S_U, and stores the token $T : (t_1, t_2) := (e_1, e_2) = (H(m), H(PkI))$.

9 $U \rightarrow I : R_U$; U sends receipt $R_U : (r_1, r_2) := (S_{PkU}(C_U), PkU)$ to I.

10 I verifies R_U. The verification is successful when the following equations are satisfied:

$$\begin{aligned} V_{r2}(C_U, r_1) &= true && (5)\\ H(r_2) &= c_1 && (6) \end{aligned}$$

Equation (5) verifies that this receipt surely corresponds to this transaction and it is surely created by the owner of r_2. Equation (6) verifies that the creator of the receipt (r_2) surely corresponds to the receiver (c_1). If the above verifications are successful, I may delete the back-up copy of E_I.

The user now has the rights definition m and a token $(H(m), H(PkI))$ stored in U. User U is then granted the rights provided in m by issuer I.

3.2.2 Transfer Transaction. The transfer transaction deletes a digital right, corresponding to m and issued by I, from user $U1$ and restores the digital right to user $U2$. This transaction is performed in the following way (Figure 6):

1 $U1 \rightarrow U2 : \{A_I, m, G_{U1}\}$; $U1$ sends its TPG $G_{U1} : (g_1, g_2) := (S_{PkG}(PkU1), PkG)$ along with A_I and m.

2 $U2$ generates a challenge $C_{U2} : (c_1, c_2) := (H(PkU2), s)$ and adds s to the session DB S_{U2}.

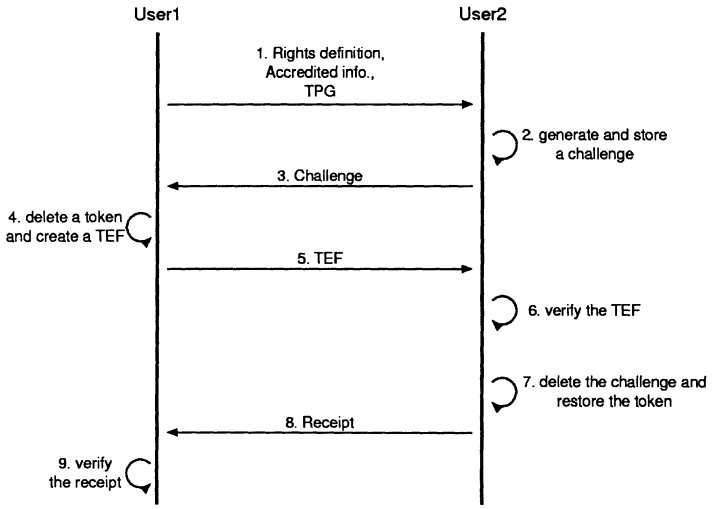

Figure 6 Transferring a digital right

3 $U2 \rightarrow U1 : C_{U2}$.

4 $U1$ deletes a stored token $T : (H(m), H(PkI))$ and generates a corresponding TEF E_{U1}, which consists of:

$$\begin{aligned} e_1 &:= H(m) \\ e_2 &:= H(PkI) \\ e_3 &:= c_1 \\ e_4 &:= c_2 \\ e_5 &:= S_{PkU2}(e_1||e_2||e_3||e_4) \\ e_6 &:= PkU2 \end{aligned}$$

$U1$ may have a back-up copy of E_{U1} as in the issue transaction and for the same reason.

5 $I \rightarrow U : E_{U1}$.

6 $U2$ verifies E_{U1}. The verification is successful when the following equations are satisfied:

$$
\begin{aligned}
e_3 &= H(PkU2) && (7)\\
e_4 &\in S_{U2} && (8)\\
V_{e6}(e_1||e_2||e_3||e_4, e_5) &= true && (9)\\
V_{g2}(e_6, g_1) &= true && (10)\\
H(g_2) &\in a_1 && (11)\\
V_{a3}(a_1, a_2) &= true && (12)\\
H(a_3) &= e_2 && (13)\\
e_2 &\in L && (14)
\end{aligned}
$$

Equations (7), (8) and (9) are verifications similar to (1), (2) and (3). Equation (10) verifies that guarantor g_2 guarantees the tamper-proof capability of sender e_6. Equations (11) and (12) verifies that g_2 is accredited by a_3. Equation (13) verifies that a_3 is certainly the issuer of the transferred token. Equation (14) verifies that the corresponding digital right is effective.

7 If the verifications above are successful, $U2$ deletes e_4 from S_{U2}, and stores the token T.

8 $U2 \rightarrow U1 : R_{U2}$.

9 $U1$ verifies R_{U2} and deletes the back-up of E_{U1} in the same manner as in the issuance stage.

The receiver now has the rights definition m and a token $(H(m), H(PkI))$, which is deleted from $U1$. This completes the transfer of the digital right.

3.2.3 Redemption Transaction. The redemption transaction between a user and a collector is performed in a similar way to the transfer transaction. The differences from the transfer transaction are as follows (Figure 7):

- The challenge C should include information that indicates whether the process is consumption or presentation; Negating c_2 to indicate presentation, for example.
- The token is deleted from the user in conjunction with the generation of a TEF only when consumption is indicated (e.g. when c_2 is a positive number).

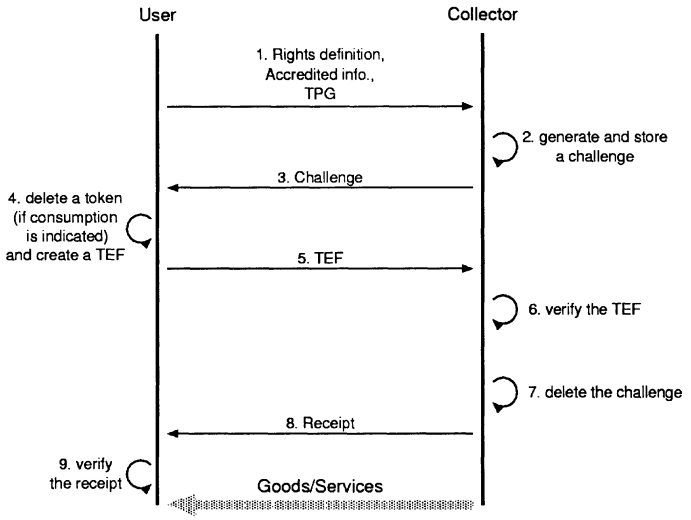

Figure 7 **Redeeming a digital right**

- After the transaction is successfully completed, the goods or services corresponding to the rights definition are provided[4] from the collector to the user.

4. DISCUSSION

This section discusses the level of security of the proposed circulation scheme. It is assumed that secret keys are managed properly without any leakage and that the tamper-proof capability of smartcards are not compromised. The latter will be discussed at the end of this section.

4.1. PREVENTING ALTERATION

To prevent the alteration of a digital right, it is necessary to prevent alteration of the rights definition and the manifest in the token.

A rights definition is hard to alter because the corresponding token has a hash value of the rights definition as a manifest. Although it is possible to alter the rights definition when hash-collision occurs, it is regarded as practically impossible when a fairly secure hash function is used. Thus, the possibility of altering the rights definition depends on the degree of security that the secure hash function provides.

The token is stored in a smartcard that is assumed tamper-proof except to be circulated as a part of TEF. Because the TEF is protected by a signature of the sender, the possibility of altering the token depends on the degree of security provided by the signature.

4.2. PREVENTING FORGERY

To prevent the forgery of a digital right, it is necessary to prevent alteration of the issuer information in a token and the creation of a token whose issuer information corresponds to a public key of the other participant.

As discussed above, the possibility of altering the token depends on the strength of the signature.

It is possible to create a token with false issuer information if the attacker can successfully pretend to be the other issuer. Since this attack is prevented by equations (3) and (4), which represent a hash and a signature, the possibility depends on the strength of the hash and that of the signature.

4.3. PREVENTING REPRODUCTION

To prevent reproduction, it is necessary to prevent the following attacks:

Reusing a TEF Restoration of a token from the TEF already used to restore the token.

Tapping a TEF Restoration of a token from the TEF sent to the other participant.

Pretending to be a trusted smartcard Creation of a valid TEF without deleting the corresponding token as a proper smartcard does.

Repudiating reception Saying "I didn't receive the digital right. Send it again."

Reusing a TEF is prevented by a challenge. If an attacker tries to reuse the TEF, the verifications provided by equations (2) or (8) will be failed because the corresponding challenge has been already deleted.

Tapping a TEF is also prevented by a challenge. If an attacker tries to restore a token from the TEF sent to the other participant, the verifications by the formula (1) or (7) will fail.

Pretending to be a trusted smartcard is prevented by the signatures of accredited information and TPG. Smartcards that can hold a digital right by a issuer are identified by accredited information and TPG, alteration of which is prevented by the signatures.

Repudiating reception is prevented by a back-up copy of a TEF. If the receiver claims not to have received a TEF, the sender may simply send the back-up copy of the TEF, since reusing the TEF is prevented as mentioned above.

4.4. ENSURING FAIRNESS

To ensure fairness in circulating rights, preventing the repudiation of circulation is necessary. According to the transactions explained in the previous section, repudiation can be prevented by the TEF on the sender's side and by the receipt on the receiver's side. Since the transactions can be retried without reproduction, fairness is ensured on the assumption that neither participant flees from the other.

This assumption is valid if the participants knows each other, or if the public keys of all participants are registered to a certain registrant and cheaters can be captured. The latter involves a trade-off with the desire to ensure privacy.

On other conditions, the fairness may be compromised when one flees in the middle of a transaction, such as a receiver terminating the transaction after receiving a TEF, for example. To ensure fairness under such conditions, a TEF and the corresponding receipt should be exchanged fairly. Although fair exchange protocols can be applied to realize this [Asokan et al., 1996], these protocols depend on some additional assumptions such as equal computational power or involvement of a trusted third party[Asokan, 1998]. Since these assumptions make the transactions complex, the trade-off between ensuring fairness in such situation and practicality should be considered carefully.

4.5. ENSURING PRIVACY

In the proposed scheme, the public key of the sender becomes available to the receiver because the signature of the sender must be verified on the receiver's side. When the history of the TEF is sent along with the digital right (as discussed below), public keys of the past owners also become known.

This is not a serious problem, since the proposed scheme uses a public key to identify a participant. There is no information linking public keys to users in the real world, if the registrants mentioned above are not established or they does not disclose the link.

A key management system that makes it difficult to link public keys in smartcards with users[Petersen and Horster, 1997], can be used to ensure a higher level of privacy.

4.6. DEPENDENCY ON TAMPER-PROOF DEVICES

The security of the proposed scheme largely depends on the tamper-proof capability of the smartcard. In comparison to public key encryption or secure hash functions, the security of the smartcard is considered easier to compromise, unfortunately. Since this scheme allows issuers to select their own trustful smartcards, the risk of a total break is hedged in systems using this scheme. However, further security measures are required in an infrastructure that circulates rights of higher value.

In addition to a mechanism that prevents illegal activities in the proposed scheme, it is possible to adopt a method of detecting illegal acts through smartcard violation by using the history of TEFs.

A TEF includes the information on the receiver's key as part of a challenge and contains the signature of the sender. By circulating the history of a TEF along with the corresponding digital right, a chain of signatures can be composed. When illegal reproduction occurs, it is possible to identify the perpetrator by finding the branching point in the chain of signatures.

The function of detecting illegal acts through violation of smartcards works as a deterrent against such acts. It is necessary, however, to note that circulating and verifying a chain of signatures place a considerable load on the system.

5. RELATED WORKS

Similar to the measures against the reproduction and duplicate-redemption of information such as digital rights that represent values, various methods are used to prevent double spending in electronic cash systems[Wayner, 1997]. They are roughly divided into the following categories:

Account book method Double spending is prevented by centrally managing an account book that records the ownership and use of electronic cash.

History verification method A circulation history is attached to electronic cash when circulated and double spending is detected by verifying the history when returned.

Balance method Electronic cash is stored in a tamper-proof device such as a smartcard. The tamper-proof device ensures that the amount of electronic cash is decreased when transferred or used and that illegally increasing the balance or double spending does not occur.

In the account book method, double spending is detected as an inconsistency in an update transaction process. Many systems including eCash[Chaum et al., 1988] and iKP[Bellare et al., 1995] use this method. This method cannot be used off-line because it requires access to the server when electronic cash is circulated; however, it is relatively easy to prevent double spending in an on-line environment, and it is possible to make payment transactions performed in off-line environment using smartcards[Brands, 1994]. A method for applying the account book method to the circulation of rights has been proposed[Matsuyama and Fujimura, 1999].

In the history verification method, double spending is detected because two different sets of electronic cash with the same identifier are returned. When double spending is detected, the perpetrator is identified by comparing the circulation history of the two sets of electronic cash and finding the branching point. The history of a token used in FlexToken corresponds to the circulation history in this electronic cash system. In this approach, however, the validity of the electronic cash is not guaranteed during circulation because double spending cannot be detected until the electronic cash is returned. To solve this problem, a method of guaranteeing the validity of cash during circulation by combining the history verification method with the balance method using a smartcard has been proposed[Nakayama et al., 1997].

In the balance method, double spending is prevented by a tamper-proof device such as a smartcard. This method is used in Mondex[Mondex International,] and some systems compliant with CEN prEN 1546 [prEN 1546, 1995]. Unlike the history verification method, the validity of electronic cash is guaranteed during circulation because double spending is prevented by the tamper-proof device. It is similar to FlexToken in its dependency on a tamper-proof device; however, the method was developed for a system that deals only with specific currencies issued by specific issuers (such as central banks) as discussed in Section 2. It is thus difficult to use the method in a rights trading infrastructure that needs to deal with a wide range of digital rights issued by various issuers.

In other areas, systems for preventing copying have been proposed for digital contents such as music and images. DigiBox[Sibert et al., 1995] is included in such systems. The purpose and mechanism of these systems differ from those the proposed scheme, which is intended to guarantee the genuineness of circulated rights definition and not meant to prevent copying of the rights definition itself, which corresponds to digital contents.

Although it is not discussed in this paper, to establish a infrastructure for trading rights, a method of describing rights definition is required in

order to define the value of the contents of rights. A rights description language called XML Ticket[Fujimura et al., 1999], which is based on a rights model that can be hierarchically structured, has been proposed. It has been confirmed on a prototype that a rights trading system can be established by preventing copying of rights information described in this language by using the proposed scheme.

6. CONCLUSION

This paper described the requirements for a copy prevention scheme for trading rights and proposed FlexToken as a system that can satisfy these requirements. It was shown that the proposed scheme handles a wide range of rights and issuers by separating the information that represents genuineness of a right from its contents. This paper also described the procedure of circulating rights and evaluated its security.

The proposed scheme enables any issuer to use pre-delivered smartcards as a copy prevention infrastructure for diverse types of digital rights.

A prototype has been produced based on the proposed scheme. The feasibility of FlexToken was verified using the prototype. We are conducting a practicality evaluation by applying the proposed scheme to admission tickets and reservation tickets for public facilities.

Acknowledgments

We wish to thank all the members of the FlexTicket project, especially Yasunao Mizuno, Yoshihito Oshima, Yoshiaki Nakajima, Nobuyuki Chiwata, Makoto Iguchi, and Jun Sekine.

Notes

1. The trust domain may vary depending on not only the issuer of rights but also by the type of rights. For example, issuers may want to circulate expensive tickets only on strongly secure (and maybe expensive) tamper-proof devices and inexpensive tickets on widely-used devices with weaker security.

2. To distinguish the effect of the signature, it is recommended that each information which has a signature is "tagged" with the meaning of the information[Aura, 1997] and the term of validity. These tags are quite important in real implementation, but are omitted for simplicity in this paper.

3. A smartcard of a user, to be exact.

4. In reality, a process in which the goods or services to be provided is determined by interpreting the contents of the rights definition, however, this process is not discussed here because it is outside the scope of this paper.

References

[Asokan, 1998] Asokan, N. (1998). Fairness in Electronic Commerce. PhD thesis, University of Waterloo.

[Asokan et al., 1996] Asokan, N., Schunter, M., and Waidner, M. (1996). Optimistic protocols for fair exchange. Technical Report RZ 2858, IBM.

[Aura, 1997] Aura, T. (1997). Strategies against replay attacks. In Proceedings of the 10th IEEE Computer Security Foundations Workshop. IEEE Computer Society.

[Bellare et al., 1995] Bellare, M., Garay, J. A., Hauser, R., Herzberg, A., Krawczyk, H., Steiner, M., Tsudik, G., and Waidner, M. (1995). iKP – a family of secure electronic payment protocols. In Proceedings of the First USENIX Workshop on Electronic Commerce.

[Brands, 1994] Brands, S. (1994). Off-line cash transfer by smart cards. Technical Report CS–R9455, CWI.

[Chaum et al., 1988] Chaum, D., Fiat, A., and Naor, M. (1988). Untraceable electronic cash. In Proceedings of Crypto 88. Springer Verlag.

[Clarke, 1996] Clarke, R. (1996). The mondex value-card scheme midterm report. In Chip-Based Payment Schemes: Stored-Value Cards and Beyond. Xamax Consultancy Pty.

[Ellison et al., 1999] Ellison, C. M., Frantz, B., Lampson, B., Rivest, R., Thomas, B., and Ylonen, T. (1999). RFC 2693: SPKI Certificate Theory. Internet Society.

[Fujimura, 2000] Fujimura, K. (2000). Requirements for Digital-Right Trading. IETF Trade Working Group. draft-ietf-trade-drt-requirements-00.txt.

[Fujimura et al., 1999] Fujimura, K., Nakajima, Y., and Sekine, J. (1999). XML Ticket: Generalized digital ticket definition language. http://www.w3.org/DSig/signed-XML99/pp/NTT_xml_ticket.html.

[Matsuyama and Fujimura, 1999] Matsuyama, K. and Fujimura, K. (1999). Distributed digital-ticket management for rights trading system. In Proceedings of the 1st ACM Conference on Electronic Commerce.

[Mondex International,] Mondex International. Mondex electronic cash. http://www.mondex.com/.

[Nakayama et al., 1997] Nakayama, Y., Moribatake, H., Abe, M., and Fujisaki, E. (1997). An electronic money scheme – a proposal for a new electronic money scheme which is both secure and convenient. In IMES BOJ Discussion Paper. Institute for Monetary and Economic Studies, Bank of Japan.

[Petersen and Horster, 1997] Petersen, H. and Horster, P. (1997). Self-certified keys - concepts and applications. In Proceedings of 3rd Conference on Communication and Multimedia Security. Chapman&Hall.

[prEN 1546, 1995] prEN 1546 (1995). Inter-sector electronic purse. Comité Européen de Normalisation.

[Sibert et al., 1995] Sibert, O., Bernstein, D., and Wie, D. V. (1995). The DigiBox: A self-protecting container for information commerce. In Proceedings of the 1st USENIX Workshop of Electronic Commerce.

[Wayner, 1997] Wayner, P. (1997). Digital Cash. AP Professional, Chestnut Hill, MA.

[Xerox Corporation, 1998] Xerox Corporation (1998). The Digital Property Rights Language Manual and Tutorial – XML Edition.