

Groupe de travail Réseau  
**Request for Comments : 3506**  
 Catégorie : Information  
 Traduction Claude Brière de L'Isle

K. Fujimura, NTT  
 D. Eastlake 3<sup>rd</sup>, Motorola

mars 2003

## Exigences et conception du système de commercialisation des bons d'échange (VTS)

### Statut de ce mémoire

Le présent mémoire donne des informations pour la communauté de l'Internet. Il ne spécifie aucune sorte de norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.

### Notice de copyright

Copyright (C) The Internet Society (2003). Tous droits réservés.

### Résumé

Créditer des points de fidélité et collecter des coupons numériques ou des certificats de cadeaux sont des fonctions courantes dans les transactions d'achat et de commerce. Ces activités peuvent être généralisées en utilisant le concept d'un "bon d'échange" (*voucher*), qui est une représentation numérique du droit de réclamer des biens ou services. Le présent document présente un système de commercialisation de bons d'échange (VTS, *Voucher Trading System*) qui assure la circulation sûre des bons d'échange, et sa terminologie ; il énumère ses principes de conception et les exigences de VTS et du langage générique des bons d'échange (GVL, *Generic Voucher Language*) avec les divers types de bons d'échange qui peuvent être décrits.

### Conventions utilisées dans ce document

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119], [RFC8174].

## Table des Matières

|   |   |
|---|---|
| 1. Fondements.....  | 2 |
| 2. Terminologie et modèle.....                                | 2 |
| 2.1 Bon d'échange.....  | 2 |
| 2.2 Participants.....   | 2 |
| 2.3 Système de commercialisation de bons d'échange (VTS)..... | 3 |
| 3. Exigences de VTS.....                                      | 3 |
| 3.1 Diverses capacités de traitement.....                     | 3 |
| 3.2 Assurer la sécurité.....                                  | 4 |
| 3.3 Assurer la praticabilité.....                             | 4 |
| 4. Portée des spécifications de VTS.....                      | 4 |
| 4.1 Protocole de commercialisation de bons d'échange.....     | 4 |
| 4.2 VTS-API.....  | 5 |
| 4.3 Langage générique des bons d'échange.....                 | 5 |
| 5. Exigences de GVL.....                                      | 5 |
| 5.1 Sémantique.....   | 5 |
| 5.2 Syntaxe.....  | 6 |
| 5.3 Sécurité.....   | 6 |
| 5.4 Efficacité.....   | 6 |
| 5.5 Coordination.....   | 6 |
| 5.6 Exemple de GVL.....                                       | 6 |
| 6. Scénarios d'application.....                               | 6 |
| 7. Questions et réponses.....                                 | 8 |
| 8. Considérations pour la sécurité.....                       | 8 |
| 9. Remerciements.....   | 8 |
| 10. Références.....   | 8 |
| 11. Adresse des auteurs.....                                  | 9 |
| 12. Déclaration complète de droits de reproduction.....       | 9 |

## 1. Fondements

Il est souvent nécessaire de créditer des points de fidélité, de collecter des coupons numériques ou des certificats de cadeaux, etc., pour compléter des achats ou autres transactions commerciales dans la vraie vie. L'importance de ces activités est aussi reconnue dans le commerce Internet. Si un système de production ou de collecte différent pour traiter de tels points ou coupons doit être développé pour chaque application individuelle, les coûts de mise en œuvre seront excessifs, paralysant l'utilisation de ces mécanismes dans le commerce électronique. Les consommateurs peuvent aussi être forcés d'installer un certain nombre de modules logiciels pour traiter ces points ou coupons.

Un bon d'échange (*voucher*) est une représentation numérique du droit de réclamer des services ou des biens. En utilisant des bons d'échange, une large gamme de valeurs électroniques, incluant des points ou coupons, peut être traitée d'une façon uniforme avec un seul module logiciel commercial.

Le présent document présente la terminologie et le modèle d'un système de commercialisation de bons d'échange (VTS, *Voucher Trading System*) qui fait circuler les bons d'échange de manière sûre ; il fait aussi la liste des principes de conception et des exigences pour un VTS et le langage générique de bons d'échange (GVL, *Generic Voucher Language*) avec lequel les divers types de bons d'échange peuvent être décrits.

## 2. Terminologie et modèle

### 2.1 Bon d'échange

Un bon d'échange est une représentation numérique du droit de réclamer des biens ou des services. Pour préciser la différence entre les bons d'échange et la monnaie électronique ou les certificats numériques, on introduit une définition formelle du bon d'échange dans ce document.

Soient I un producteur de bon d'échange, H un détenteur de bon d'échange, P la promesse du producteur au détenteur du bon d'échange. Un bon d'échange est défini par le triplet  $\langle I, P, H \rangle$ .

Voici des exemples de P :

- o Deux points de fidélité sont ajoutés par achat à une carte. Si vous collectez 50 points, vous obtiendrez un article gratuitement (points de fidélité).
- o Déduisez 10 % du total de vos achats sur présentation de cette carte (carte d'adhésion).
- o Déduisez 50 % du total de vos achats avec ce coupon. La transaction d'achat consomme le coupon (coupon).
- o Le porteur peut avoir accès à "http://..." gratuitement pendant un mois (ticket gratuit pour une promotion des ventes).
- o Le porteur peut échanger ce ticket contre les vêtements commandés (ticket d'échange ou bulletin de livraison).
- o Le siège numéro A-24 a été réservé pour le "concert X" le 2 avril (ticket d'événement).

Noter que P n'a pas besoin d'être décrit en termes de langage naturel du moment que le contenu du bon d'échange est spécifié. Par exemple, un ensemble de paires de nom d'attribut et de valeurs décrites en XML peut être employé pour définir le contenu.

### 2.2 Participants

Il y a quatre types de participants dans le modèle de commercialisation de bons d'échange : le producteur, le détenteur, le collecteur, et le fournisseur du VTS. Leurs rôles sont les suivants :

Producteur : il crée et produit un bon d'échange. Il garantit le contenu du bon d'échange.

Détenteur (ou utilisateur) : il possède le bon d'échange. Il transfère et rachète le bon d'échange à d'autres utilisateurs ou au collecteur.

Collecteur (ou vérificateur) : il collecte ou vérifie le bon d'échange et met en œuvre sa promesse. En général, il est compensé par des biens ou des services rendus.

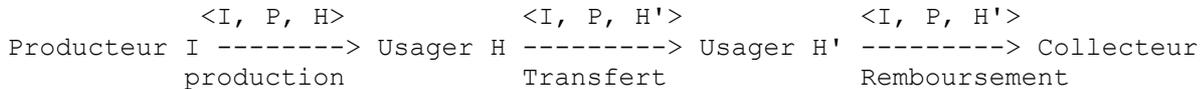
Fournisseur de VTS : il fournit un VTS et garantit qu'un bon d'échange particulier n'est pas alloué à plusieurs détenteurs ou utilisé plusieurs fois sauf permis pour ce type de bon d'échange.

Le modèle IOTP [RFC2801] inclut des marchands, des livreurs, des consommateurs et d'autres participants. Ils jouent divers rôles dans le système parce qu'un marchand, par exemple, peut être considéré comme producteur, ou détenteur selon

que le marchand crée lui-même le bon d'échange ou l'achète d'un grossiste ou d'un fabricant. Un marchand peut aussi être un collecteur si la boutique collecte les certificats ou coupons cadeaux.

### 2.3 Système de commercialisation de bons d'échange (VTS)

Un bon d'échange est généré par le producteur, est commercialisé parmi les détenteurs (utilisateurs) et finalement est collecté par le collecteur :



**Figure 1 : cycle de vie des bons d'échange**

Le fournisseur de VTS fournit un VTS qui permet que des bons d'échange circulent en toute sécurité parmi les participants.

Voici une définition formelle du VTS : un système de commercialisation de bons d'échange (VTS) est un système qui gère de façon logique un ensemble de bons d'échange valides (VVS) qui est un sous ensemble de  $\{\langle I, P, H \rangle \mid I \text{ dans IS, } P \text{ dans PS, } H \text{ dans HS}\}$  où IS est l'ensemble des producteurs, PS est l'ensemble des promesses, et HS est l'ensemble des détenteurs ; le VTS les empêche d'être modifiés ou reproduits sauf par les trois transactions suivantes : production, transfert, et remboursement. L'état initial du VVS est un ensemble vide.

Noter que cela n'implique pas que VVS soit mémorisé physiquement dans une base de données centralisée. Par exemple, une mise en œuvre peut mémoriser des bons d'échange dans des cartes à mémoire réparties portées par le détenteur [T00], ou peut les mémoriser dans plusieurs serveurs gérés par chaque producteur ou des tiers de confiance. Ceci est une politique de confiance et/ou une question de mise en œuvre [MF99].

**Production** : une transaction de production est l'action qui crée le triplet  $\langle I, P, H \rangle$  et l'ajoute au VVS avec les intentions du producteur.

**Transfert** : une transaction de transfert est l'action qui réécrit le triplet  $\langle I, P, H \rangle$  (dans le VVS) comme  $\langle I, P, H' \rangle$  ( $H \diamond H'$ ) pour refléter les intentions du détenteur original de H.

**Remboursement** : il y a deux transactions de remboursement : présentation et consommation.

Une transaction de présentation est l'action qui montre le triplet  $\langle I, P, H \rangle$  (dans le VVS) pour refléter les intentions du détenteur de H. Dans ce cas, la propriété du bon d'échange est conservée quand le bon d'échange est remboursé, par exemple, restitution (présentation) de licences ou passeports.

Une transaction de consommation est l'action qui supprime le triplet  $\langle I, P, H \rangle$  (dans le VVS) pour refléter l'intention du détenteur de H et les propriétés du bon d'échange. La propriété du bon d'échange peut être annulée, ou le nombre de fois qu'il est valide réduite lorsque le bon d'échange est remboursé, par exemple, le remboursement de tickets d'événement ou de cartes de téléphone.

Noter que une ou plusieurs de ces transactions peuvent être exécutées au titre de la même transaction d'achat IOTP. Voir les détails à la Section 6.

## 3. Exigences de VTS

Un VTS doit satisfaire aux exigences suivantes :

- (1) Il DOIT traiter divers types de bons d'échange produits par différents producteurs.
- (2) Il DOIT empêcher des actes illégaux comme l'altération, la falsification, et la reproduction, et assurer la confidentialité.
- (3) Il DOIT être praticable en termes de coûts et efficacité de mise en œuvre/fonctionnement.

Chacune de ces exigences est discutée en détail ci-dessous.

### 3.1 Diverses capacités de traitement

- (a) Différents producteurs : à la différence du système de monnaie numérique qui ne traite que la monnaie produite par un producteur spécifique comme une banque centrale, le système de commercialisation de bons d'échange DOIT traiter les

bons d'échange produits par plusieurs producteurs.

- (b) Divers types de bons d'échange : à la différence d'un système de monnaie numérique qui ne traite qu'une monnaie, le système DOIT traiter divers types de bons d'échange, comme des certificats de cadeaux, des coupons, et des points de fidélité.

### 3.2 Assurer la sécurité

- (c) Empêcher la falsification : seul le producteur peut causer la production d'un bon d'échange valide. Il NE DOIT PAS être possible à d'autres parties de causer la création d'un bon d'échange valide.
- (d) Empêcher l'altération : le bon d'échange NE DOIT PAS être altéré durant la circulation, mais la transaction de transfert, dans laquelle le détenteur du bon d'échange est réécrit, est permise. Seul le détenteur actuel peut initier une transaction de transfert.
- (e) Empêcher la duplication-remboursement : un bon d'échange NE DOIT PAS être remboursable une fois qu'il a été consommé (le résultat de transactions de remboursement). Seul le détenteur peut initier une transaction de remboursement.
- (f) Empêcher la reproduction : un bon d'échange NE DOIT PAS être reproduit pendant qu'il est en circulation. C'est à dire qu'il doit y avoir seulement un détenteur valide de tout bon d'échange particulier à un instant donné.
- (g) Non répudiation : il NE DEVRAIT PAS être possible au producteur de répudier sa production, ou au détenteur de répudier le transfert ou le remboursement d'un bon d'échange, après qu'il a été produit, transféré ou remboursé.
- (h) Assurer la confidentialité : les détenteurs actuels et précédents d'un bon d'échange DEVRAIENT être dissimulés à ceux qui entrent en possession du bon d'échange.
- (i) Gestion de la confiance : si une grande variété de bons d'échange est en circulation, il peut être difficile aux usagers de juger si un bon d'échange peut être cru ou non. Pour aider ces usagers, une fonction de gestion de confiance qui vérifie l'authenticité d'un bon d'échange DEVRAIT être prise en charge.

### 3.3 Assurer la praticabilité

- (j) Adaptabilité : un seul courtier centralisé qui vend tous les types de bons d'échange, ou une autorité centralisée qui authentifie tous les producteurs ou autres participants, NE DEVRAIT PAS être supposé. Un système qui s'appuie sur une seule organisation centralisée est excessivement fragile ; une défaillance dans cette organisation cause un échec complet du système.
- (k) Efficacité : il DOIT être possible de mettre en œuvre un VTS de façon efficace. De nombreuses applications de bons d'échange, par exemple, un ticket d'événement ou un passe de transport, exige de bonnes performances, en particulier lorsque le bon d'échange est remboursé.
- (l) Simplicité : il DEVRAIT être possible de mettre en œuvre VTS de façon simple. La simplicité est importante pour réduire le coût de mise en œuvre. Elle est aussi importante pour comprendre le système, ce qui est nécessaire pour la confiance dans le système.

## 4. Portée des spécifications de VTS

Pour mettre en œuvre un VTS, le protocole de commercialisation de bons d'échanges (VTP, *Voucher Trading Protocol*), l'interface de programmation d'application VTS (VTS-API, *VTS Application Programming Interface*), et le langage générique de bons d'échange (GVL, *Generic Voucher Language*) doivent être développés. Les objectifs, avantages, et limitations de la normalisation de chaque spécification sont discutés ci-dessous.

### 4.1 Protocole de commercialisation de bons d'échange

Pour réaliser l'interopérabilité parmi plusieurs VTS développés par des fournisseurs de VTS indépendants, des protocoles standard pour la production, le transfert, ou le remboursement des bons d'échange seront nécessaires. Cependant, il y a plusieurs façons de mettre en œuvre des VTS. Pour des coupons de réduction ou des tickets d'événement, par exemple, le

VTS hors ligne décentralisé fondé sur la carte à mémoire est souvent préféré, tandis que pour les bons ou titres, le VTS en ligne centralisé peut être préféré. Il n'est pas possible de définir de protocole standard pour l'instant.

## 4.2 VTS-API

Pour donner aux producteurs et développeurs d'application une certaine liberté en termes de choix de VTS, il devrait être spécifié une interface de programmation d'application de VTS (VTS-API) standard qui puisse encapsuler les mises en œuvre de VTS. Cela permet à une application appelante de produire, transférer, et rembourser le bon d'échange d'une manière uniforme indépendamment de la mise en œuvre de VTS. Les fonctions de base, c'est-à-dire la production, le transfert, et le remboursement, fournis par VTS-API peuvent être directement dérivés du modèle VTS décrit dans le présent document. Plus de détails de conception de VTS-API seront discutés dans un document séparé ou une spécification VTS-API séparée [RFC4154].

## 4.3 Langage générique des bons d'échange

Pour satisfaire aux diverses exigences de VTS (voir la Section 3) on devrait spécifier un langage générique de bons d'échange (GVL) standard qui concrétise les diverses propriétés de bon d'échange. Cette approche assurerait que VTS est indépendant de l'application. Le langage devrait être capable de définir les diverses promesses P du bon d'échange <I, P, H> de couvrir les tickets, coupons, points de fidélité, et certificats de cadeaux de façon uniforme. Spécifier I et H est une question de mise en œuvre de VTS qui peut être réalisée en utilisant une clé publique, un hachage d'une clé publique, un URI ou d'autres noms avec une règle de délimitation.

Dans la section qui suit, on discute en détails des exigences de GVL.

# 5. Exigences de GVL

## 5.1 Sémantique

La sémantique prise en charge par le langage et ses niveaux d'exigence sont décrits en détails ci-dessous.

- (a) Contrôle de validité : la méthode d'invalidation (oblitération) qui est exécutée lorsque le bon d'échange est remboursé dépend du type du bon d'échange. Par exemple, un point de fidélité sera invalidé si le point est remboursé mais une carte de membre peut être utilisée de façon répétée sans considération du nombre de fois qu'elle est présentée. Le langage DOIT être capable de définir comment la validité est modifiée. De plus, le langage DOIT être capable de définir la période de validité, la date de début et la date de fin.
- (b) Contrôle de transférabilité : certains types de bons d'échange exigent de pouvoir être transférés. Le langage DOIT être capable de spécifier si un bon d'échange peut être transféré.
- (c) Contrôle de circulation : selon le type de bon d'échange, diverses exigences ou restrictions de circulation doivent être satisfaites [F99], par exemple, seulement des boutiques qualifiées peuvent produire des bons d'échange particuliers ou seulement un certain fournisseur de service peut oblitérer (invalider) certains bons d'échange. Le langage DEVRAIT être capable de spécifier de telles exigences de circulation.
- (d) Contrôle de l'anonymat : différents types de bons d'échange vont exiger des niveaux différents d'anonymat. Le langage DEVRAIT être capable de réaliser le niveau d'anonymat requis.
- (e) Compréhensibilité : les termes et la description d'un bon d'échange DEVRAIENT être objectivement compréhensibles par les participants, parce que cela contribuera à réduire le nombre de conflits sur l'interprétation des promesses des bons d'échange.
- (f) Gestion de l'état : certains types de bons d'échange ont des propriétés dont la valeur peut changer de façon dynamique avec leur circulation, par exemple, l'état de paiement, l'état de réservation, ou l'état d'approbation. Le langage PEUT prendre en charge la définition de telles propriétés.
- (g) Composabilité : certains types de bons d'échange consistent en plusieurs sous bons d'échange, qui peuvent être produits séparément des bons d'échange originaux normalement parce que les bons d'échange sont produits par différentes organisations ou produits à des moments différents. Le langage PEUT prendre en charge des bons d'échange composés de plusieurs sous bons d'échange.

## 5.2 Syntaxe

Pour assurer la cohérence avec les autres normes en rapport désignées ci-dessous, la syntaxe du langage DOIT se fonder sur le langage de balisage extensible [XML].

La syntaxe du langage DOIT permettre de définir toutes les propriétés spécifiques d'application, par exemple un numéro de siège, un numéro de vol, etc.. Un langage de définition de schéma qui puisse être traduit en déclarations de type de données (DTD) spécifiques d'application peut être nécessaire.

## 5.3 Sécurité

Le langage DOIT fournir les paramètres nécessaires pour assurer la sécurité. Les exigences de sécurité suivent cependant principalement les exigences de VTS décrites à la Section 3 plutôt que les exigences de GVL.

## 5.4 Efficacité

Les bons d'échange peuvent être mémorisés dans une carte à mémoire ou une tablette avec une quantité de mémoire restreinte. Les grandes définitions peuvent impliquer de longs délais de transfert et de traitement, qui peuvent n'être pas acceptables. Le langage DEVRAIT permettre une définition efficace des bons d'échange

## 5.5 Coordination

La spécification du langage DEVRAIT être cohérente avec les spécifications suivantes :

- (1) Protocole Internet du commerce ouvert v1.0 [RFC2801]
- (2) Signatures XML [XMLDSIG]
- (3) Recommandation du langage de balisage extensible (XML) [XML]
- (4) Langage de modélisation du commerce électronique (ECML) version 2 [RFC4112]

## 5.6 Exemple de GVL

Un exemple de définition de bon d'échange en GVL est décrit ci-dessous. Cet exemple définit un coupon de réduction de cinq Euros pour une marchandise spécifique, un livre avec le numéro ISBN 0071355014. Ce coupon circule en utilisant un VTS appelé "Échangeur de bons". Pour réclamer cette offre, on doit dépenser un coupon. Le coupon est valide du 1<sup>er</sup> avril 2001 au 31 mars 2002.

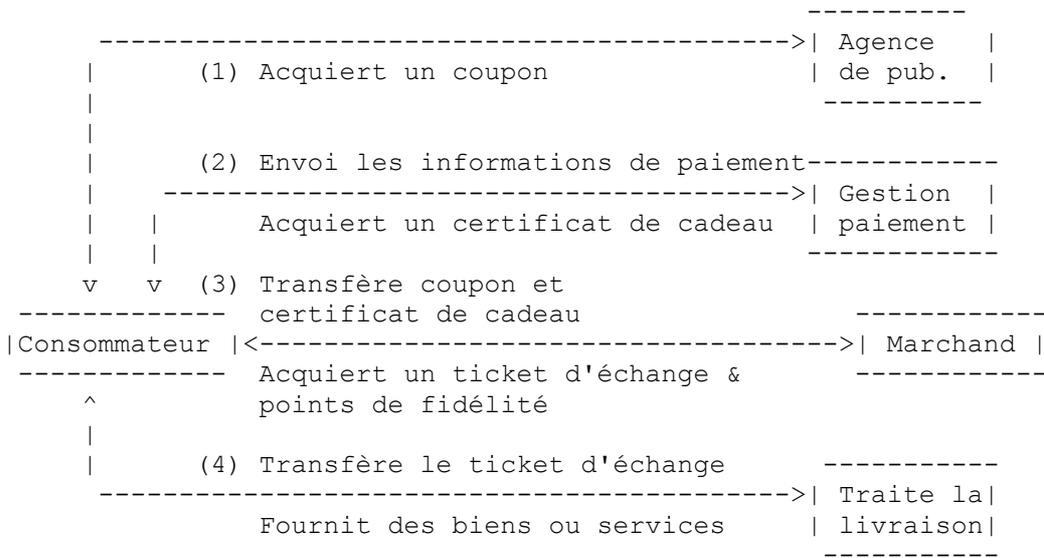
```
<?xml version="1.0"?>
<Voucher xmlns="urn:ietf:params:xml:schema:vts-lang"
  xmlns:vts="http://www.exemple.com/vts">
  <Titre>Coupn de livre IOTP</Titre>
  <Description>5 € de réduction sur le livre IOTP</Description>
  <Nom du fournisseur="Échangeur de bons">
    <vts:Version>VE2.31</vts:Version>
  </Fournisseur>
  <Type de valeur ="réduction" dépense="1">
    <Quantité fixe="5" monnaie="EUR"/>
  </Valeur>

  <Marchandise>
    <bk:livre xmlns:bk="http://www.exemple.com/bk"
      bk:isbn="0071355014"/>
  </Marchandise>
  <ValidPeriod début="2001-04-01" fin="2002-03-31"/>
</Voucher>
```

## 6. Scénarios d'application

Cette Section décrit à titre d'exemple typique de commerce électronique avec des transactions d'annonce, de paiement, et de livraison, l'utilisation de bons d'échange et de VTS, et montre que les bons d'échange peuvent être utilisés comme moyen efficace de coordonner des services autonomes qui n'ont pas encore établi de relation de confiance les uns avec les autres.

La Figure 2 montre un exemple typique de commerce électronique d'un consommateur qui cherche des biens ou services et fait un achat :



**Figure 2 : exemple d'application de bons d'échange**

- (1) Utilise un moteur de recherche pour trouver les biens ou services désirés et acquérir un coupon d'une agence qui représente le droit d'acheter les biens ou services avec une réduction de prix.
- (2) Acquiert un certificat de cadeau de la part d'un traitement de paiement en échange de moyens ou informations de paiement.
- (3) Transfère le coupon et le certificat de cadeau au marchand, et en échange acquiert un ticket d'échange et des points de fidélité.
- (4) Transfère le ticket d'échange au livreur, de qui il reçoit les biens ou services.

Dans cet exemple, le coupon, le certificat de cadeau, et le ticket d'échange représentent chacun le support qui donne les quatre transactions ci-dessus.

Noter qu'il n'est pas nécessaire de faire confiance aux participants impliqués dans les transactions, mais de faire confiance aux bons d'échange eux-mêmes. En d'autres termes, il n'est pas besoin de souscrire des contrats à l'avance entre les participants si les bons d'échange eux-mêmes sont fiables.

En prenant l'exemple du ticket d'échange, même si le livreur ne fait pas confiance au consommateur, le marchand qui a produit le ticket d'échange est de confiance, et si le VTS garantit qu'il n'y a pas de duplication dans le processus commercial du ticket d'échange, il n'y a pas de problème à troquer le ticket d'échange contre les biens ou services. De la même façon, même si le commerçant ne fait pas confiance au traitement de la livraison, la production du ticket d'échange peut être vérifiée, et si le VTS garantit qu'il n'y a pas de duplication dans le processus de commercialisation du ticket d'échange, il n'y a pas de problème à troquer le ticket d'échange contre les biens ou services (Figure 3). En d'autres termes, si il y a de la confiance dans le producteur et dans le VTS, la confiance entre les participants impliqués dans les transactions n'est pas nécessaire.



**Figure 3 : coordination de participants qui ne sont pas de confiance, avec ticket d'échange**

En général, il est plus difficile de faire confiance aux individus qu'aux entreprises, de sorte que cette caractéristique de VTS est particulièrement importante.

De plus, les transactions qui impliquent des bons d'échange ont des caractéristiques désirables par rapport à la protection de la confidentialité. Par exemple, dans le scénario d'échange de ticket ci-dessus, le consommateur peut désigner le service de livraison pour lui-même, de sorte que le commerçant n'a même pas besoin de connaître la moindre information personnelle comme l'adresse de livraison. De surcroît, en désignant un magasin convenable, etc., comme point de réception, le service de livraison n'a pas besoin de connaître l'adresse du consommateur.

## 7. Questions et réponses

- Est-il possible de mettre en œuvre un VTS en utilisant des certificats numériques ?  
Si la transférabilité n'est pas exigée, un bon d'échange peut facilement être mis en œuvre comme un certificat numérique, c'est-à-dire, Signed\_I(I, P, H), où la phrase "Signed\_I" signifie que le bloc entier est signé par la signature numérique du producteur. Si la transférabilité est requise, H est alors changé durant le transfert, c'est-à-dire, la signature est cassée. De plus, une vérification en ligne de base de données ou un appareil résistant aux altérations est nécessaire pour empêcher la duplication du remboursement.
- Quelle est la différence avec la monnaie numérique ?  
Un VTS doit traiter divers types de bons d'échange, comme des certificats de cadeau, des coupons, ou des points de fidélité, à la différence d'un système de monnaie numérique qui traite seulement des devises. De plus, les bons d'échange sont produits par des producteurs différents.
- Est-il possible de prendre en charge des "droits de propriété numériques" ?  
Les droits de propriété numériques peuvent être représentés comme des bons d'échange et peuvent être commercialisés en utilisant un VTS. Cependant, certains systèmes de rendu protégés seraient nécessaires pour régénérer en toute sécurité le contenu numérique afin de prendre en charge les droits de propriété numériques. Ces exigences sortent du domaine d'application des VTS.

## 8. Considérations pour la sécurité

Les questions de sécurité sont traitées aux paragraphes 3.2 et 5.3.

## 9. Remerciements

Merci à Masayuki Terada et Perry E. Metzger de leurs précieux commentaires.

## 10. Références

- [F99] K. Fujimura, H. Kuno, M. Terada, K. Matsuyama, Y. Mizuno, and J. Sekine, "Digital-Ticket-Controlled Digital Ticket Circulation", 8th USENIX Security Symposium, août 1999.
- [MF99] K. Matsuyama and K. Fujimura, "Distributed Digital-Ticket Management for Rights Trading System", 1st ACM Conferences on Electronic Commerce, novembre 1999.
- [RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. (MàJ par [RFC8174](#))
- [RFC2801] D. Burdett, "Protocole Internet du commerce ouvert - IOTP version 1.0", avril 2000. (*Information*)
- [RFC4112] D. Eastlake 3rd, "Spécification de la version 2 du langage de modélisation du commerce électronique (ECML) version 2", juin 2005. (MàJ [RFC3106](#)) (*P.S.*)
- [T00] M. Terada, H. Kuno, M. Hanadate, and K. Fujimura, "Copy Prevention Scheme for Rights Trading Infrastructure", 4th Smart Card Research and Advanced Application Conference (CARDIS 2000), septembre 2000.
- [XML] Recommendation W3C, "Extensible Mark Up Language (XML) 1.0 (Second Edition)", octobre 2000. <<http://www.w3.org/TR/REC-xml>>.

[XMLDSIG] Proposition de recommandation W3C, "XML-Signature Syntax and Processing", août 2001.  
<<http://www.w3.org/TR/xmlsig-core>>.

## 11. Adresse des auteurs

Ko Fujimura  
NTT Corporation  
1-1 Hikari-no-oka  
Yokosuka-shi  
Kanagawa, 239-0847 JAPAN  
téléphone : (0)468-59-3814  
Fax : (0)468-59-8329  
mél : [fujimura@isl.ntt.co.jp](mailto:fujimura@isl.ntt.co.jp)

Donald E. Eastlake 3rd  
Motorola  
155 Beaver Street  
Milford, MA 01757 USA  
téléphone : 508-851-8280  
mél : [Donald.Eastlake@motorola.com](mailto:Donald.Eastlake@motorola.com)

## 12. Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2003).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et à [www.rfc-editor.org](http://www.rfc-editor.org), et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations y contenues sont fournies sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations ci-encloses ne violent aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

### Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à <http://www.ietf.org/ipr> .

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à [ietf-ipr@ietf.org](mailto:ietf-ipr@ietf.org) .

### Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par la Internet Society.