A Secure Universal Loyalty Card

Sébastien Canard[1], Fabrice Clerc[1] and Benjamin Morin[2]

[1] France Telecom R&D, 42, rue des Coutures, BP6243, 14066 Caen Cedex 4, France

[2] Supelec Rennes, Avenue de la Boulaie, BP 81127, 35511 Cesson-Sévigné Cedex, France

Abstract. In this paper, we propose a generic loyalty system based on smart cards which may be implemented in existing devices like cell phones or PDAs. Our loyalty system is secure and offers some desirable features both to customers and vendors, and may further the adoption of such win-win marketing operations. In particular, the system, reliable for both parties, is universal in the sense that there is a one-to-many relationship between a customer's loyalty card and the vendors.

1 Introduction

A loyalty program is a win-win marketing operation which consists in rewarding customers' loyal behavior. Both parties benefit from loyalty strategies: vendors conceive loyalty programs as an interesting opportunity to improve customers spending and retention while customers benefit from discounts as they purchase goods. Loyalty strategies typically rely on loyalty cards or coupons used to register customers purchases. Customers are awarded when some conditions on their past purchases is met, depending on the vendor's specific loyalty strategy. In this paper, we propose an electronic loyalty system, whose features support several factors which influence the success of loyalty strategies [8], both from the customers' and vendors' point of view. We place a great emphasis on the security of the system, which is based on smart cards technology. We identify four desirable features.

- **Universality:** vendors generally propose their own loyalty card, which is not practical for customers, who are reluctant to burden with several loyalty cards. Allowing customers use the same loyalty card to register their purchases at any vendor's may encourage them to become new customers. This characteristic is interesting for vendors because it is more challenging to obtain a new customer than to keep a current one [8].
- **Security and privacy:** the system should be reliable for both parties, *i.e.* prevent actors from cheating. We then consider various security properties such as transaction unforgeability and non repudiation, multiple dipping prevention and protection of transactions. Users are also more and more concerned about their privacy and fear that such systems infringe it. Indeed, merchants use loyalty strategies to customize their offers by performing customer profiling, *i.e.* record their past purchases, and data about their preferences and behavior. Thus, the system should preserve customers' privacy, while allowing vendors to perform pseudonymous profiling. Security requirements are described more accurately thereafter.

Canard S., Clerc F. and Morin B. (2006).
A Secure Universal Loyalty Card.
In *Proceedings of the 4th International Workshop on Security in Information Systems*, pages 13-22

- **Partnerships support:** the loyalty system should allow merchants to organize partnerships, *i.e* common loyalty operations, in order for customers to benefit from discounts when purchases are made at any of the partnership participants' shop. This feature also naturally supports corporation-wide loyalty strategies, because corporations can be seen as a specific kind of partnership. This allows customers to benefit of their discounts, independently of the shop where their purchases are made.
- **Loyalty strategy independence:** loyalty strategies define which conditions should be fulfilled by customers so as to benefit from their advantages. Several possibilities exist, depending on the vendor's objectives (*e.g.* maximize the number of purchases). Because of the universality feature, the loyalty system should support any loyalty strategy. In our approach, a loyalty strategy is implemented in a loyalty program, which is considered as a parameter of the system, so any kind of loyalty strategy shall be used, provided that the data required to compute the discount are available.
- **Low cost and ease of use:** it is important that the loyalty system be cheap, simple to install and administrate. If the loyalty system entails a management overhead and is too costly, then vendors will not use it. The universality of the loyalty system also contributes to this feature.

The aim of our paper is to create a system where each customer owns a loyalty device such as a mobile phone which permits her to participate to a loyalty operation defined by some merchant and such that this system is secure both from the merchant and the customer's viewpoint.

The paper is organized as follows: we first describe the security requirements we identified, and give an overview of our solutions. Section 3 sketches the architecture and the interactions of our system. Before concluding, we discuss the limitations of our approach and evoke related work.

2 Security Properties of the Loyalty System

The universality feature reinforces the security requirements of a loyalty system. Indeed, by using a universal loyalty system, merchants do not have the hand over the loyalty program as a whole, so they need to trust the loyalty system. Moreover, customers are more and more concerned about their privacy and want their personal data to be kept secret, so they also need to trust the loyalty system. Our loyalty system basically consists in storing the transactions between a customer and a merchant on the customer's loyalty device. Rewards are computed from the past transactions stored on the customer's loyalty device. In order to guarantee the security of our system, the storage and access to the transactions on the loyalty device requires some specific properties. We have identified five main security requirements. In the remainder of this section, we describe each of them and sketch our solution.

2.1 Transaction Unforgeability

Requirement. This states that a customer should not be able to create fake transactions to benefit from discounts illegitimately. Creating fake transactions includes 1) creating a transaction from scratch, 2) duplicating a legitimate transaction in order to benefit from a better reward and 3) make a third party customer benefit from discounts.

Solution. Eeach transaction stored on a loyalty device should be signed by the merchant in order to prevent a customer from creating fake transactions from scratch. Thereby, a merchant can check that the transactions are legitimate before awarding a customer. To prevent a customer from duplicating an existing entry, transactions include a unique identifier so that a merchant can check that several transactions with the same identifier do not exist on the customer's loyalty device. A customer could still copy her own transactions on another customer's loyalty device to let her benefit from her advantages. To prevent this, transactions also include a customer's identifier that is stored in the loyalty device. This way, a merchant can check that a customer is the owner of a transaction stored on her loyalty device by verifying that the corresponding identifier is the same as the one embedded in the loyalty device.

2.2 Non Repudiation of a Transaction

Requirement. A merchant should not be able to deny the fact that she has made a transaction with a customer. Notably, together with the unforgeability of transaction, non repudiation allows us to use the loyalty system as an estimates and receipts secure storage device (see Section 5).

Solution. Non repudiation is easily verified by the signature of the merchant in all transactions. We can imagine that the customer's terminal can verify this signature online. Nevertheless, in the case of a partnership (*i.e.* a group of merchants organizing a common loyalty strategy), one should notice that a customer can only prove that he has purchased a goods at one of the vendor's involved in the partnership, but cannot identify it. In other words, this is not an individual non repudiation.

2.3 Customers' Privacy

Requirement. This requirement states that the loyalty system should disclose as little information as possible in order not to infringe the customers' privacy. We may distinguish two kinds of information to be protected.

- Customer transactions: a merchant should solely have access to the transactions made between a given customer and himself or one of its partners. The owner of a loyalty card should have access to all her transactions stored on the loyalty device, in order to check whether she can benefit from a reward.
- Customer personal data: the system should provide anonymity of transactions, while still allowing merchants to perform "anonymous profiling". In some cases, customers may accept to disclose some of their personal data (*e.g.* name, address, etc.) in order to receive special offers from the merchant for instance. However, in this case, the system must still prevent a merchant from disclosing the customer's personal data to a third-party merchant.

Solution. Transactions are stored twice in the loyalty device. One version is encrypted by the merchant, the other by the customer. This way, a customer can decrypt any transactions and any merchant of a given partnership shall only decrypt the transactions previously encrypted by any merchant of this partnership. We assume that the customer's personal data are encrypted on the loyalty device. Thus, accessing these data requires an authentication of the customer (*e.g.* a PIN code). As stated above, transactions contain a customer identifier. Actually, a customer owns one distinct identifier for each merchant, called a *pseudonym*. Pseudonyms are used to prevent merchants from sharing the links between customers' identity and their personal data (*e.g.* name and address) with other merchants. Merchants can perform anonymous profiling since a customer always has the same pseudonym for a given merchant (see also Section 4).

2.4 Multiple Dipping Prevention

Requirement. This requirement states that a customer should not be able to take advantage of the same transaction to benefit from a discount multiple times. This requirement is optional because some loyalty strategies allow multiple dipping.

Solution. In our system, a transaction includes a counter which allows merchants to check how many times a transaction has been used to take advantage of a reward. An illegitimate multiple dipping is not possible since the customer cannot modify a transaction to change the counter, which would imply to forge the merchant's signature. The merchant updates the counter every time a transaction is used. Another possibility for the customer to fraud would be to backup a list of transactions before taking advantage of a reward, and copy them back on her loyalty device. This kind of fraud can be avoided if we assume that the loyalty device has some access control embedded which only allows a merchant to store transactions on a loyalty device (a customer is not allowed to write on her memory's device). Thus, merchant's terminal has to be authenticated by the loyalty device for a transaction to be stored (see also Section 4).

2.5 Transaction Deletion

Requirement. This requirement states that a merchant should not be able to remove transactions from a customer's loyalty card in order no to let customers enjoy their advantages. Only the owner of the loyalty card is allowed to remove transaction records from her loyalty device.

Solution. Using the access control mechanism evoked above, deleting transactions requires an authentication by the owner of the loyalty device. Another possibility for a customer would be to sign a print of all transactions stored in her device using a Message Authentication Code (MAC) with a secret key embedded in the smart card, each time a new entry is written in her device.

3 A Loyalty Card System

Our system needs the use of some basic (standard) cryptographic tools, such as a signature scheme [7] and a symmetric encryption scheme [1]. In this section, we give some definitions, we present the global architecture and the interactions to create a new transaction and to obtain an advantage.

3.1 Actors and Components of the System

Actors. There are two main actors in our system: the customer and the merchant. A merchant may be an individual or a group of vendors organizing a common loyalty operation together, called a *partnership*. Merchants are identified using an identifier denoted by $\mathcal{M}$. In the case of partnerships, merchants share a common identifier. Thus, each merchant owns at least her own identifier, plus the identifiers of the partnerships she is involved in. As stated above, customers have one identity per merchant. A customer identity for a given merchant $\mathcal{M}$ (*i.e.* a pseudonym) is denoted by $\mathcal{C}^{\mathcal{M}}$. Pseudonyms are randomly generated the first time a customer makes a purchase at a vendor's and stored in the customer's loyalty device in order to be re-used for the next purchases. This allows merchants to perform pseudonymous profiling.

Loyalty strategies and programs. A loyalty strategy is a set of rules that must be satisfied for a customer to enjoy her advantages and the nature of the corresponding discount, *e.g.* 5% of the last 10 purchases. A *loyalty program* is an implementation of a loyalty strategy which takes as input a set of transactions and outputs a discount.

Transactions. A *transaction* is an interaction between a merchant and a customer. A transaction is modeled as a tuple which contains at least a unique transaction identifier $\mathcal{T}$, a customer identifier $\mathcal{C}^{\mathcal{M}}$, a merchant identifier $\mathcal{M}$ and a counter s. The counter s is used to indicate how many times a given transaction has been dipped into by a customer to benefit from a reward. A transaction may also contain additional data related to the characteristics of goods purchased by the customers, such as a good identifier (*e.g.* the bar code), a number of goods, the amount of the transaction and the date of the transaction. These data are used by a loyalty programs to compute discounts.

Customer's loyalty device. We assume that a customer owns a loyalty device, which is composed of a memory and a smart card that can perform cryptographic operations. We assume that this memory is protected in such a way that the customer cannot write on it and a merchant cannot delete any entry (see also Sections 3.2 and 4). We also assume that the access to the personal data (name, address, etc.) are protected by a PIN code, only known by the customer. A loyalty device contains a symmetric encryption keys $\mathcal{C}^K$, a table of pseudonyms $(\mathcal{M}, \mathcal{C}^{\mathcal{M}})$, a list of *transaction records* made by the customer (see below), as well as some personal data of the customer that can be encrypted using $\mathcal{C}^K$. We here use a symmetric encryption scheme since, in the solution described below, only the loyalty device has to encrypt and decrypt transactions. A loyalty card may be implemented in an ad-hoc card or a cell phone.

Merchant's terminal. A merchant owns a terminal equipped with a memory and a processor in order to run loyalty programs. A terminal may host several loyalty programs so that the merchant can choose, when a customer can benefit from an advantage and which loyalty strategy is the best or the most relevant. Terminals are equipped with some means to interact with the customers' loyalty device, such as a smart card reader, or NFC device. In the remainder, we also assume that terminals are able to authenticate themselves with customer's devices, using standard techniques such as a PKI. Terminal authentication is required to control access to the memory of the loyalty devices. The terminal's memory stores, in a secure way (*e.g.* using a TPM) a set of tuples $P = \{(\mathcal{M}_1, \mathcal{M}_1^{K_s}, \mathcal{M}_1^{K_p}, \mathcal{M}_1^{K}), \cdots, (\mathcal{M}_n, \mathcal{M}_n^{K_s}, \mathcal{M}_n^{K_p}, \mathcal{M}_n^{K})\}$, where $\mathcal{M}_i$ is a partnership identifier, $\mathcal{M}_i^{K_s}$ is the partnership's shared signature key, $\mathcal{M}_i^{K_p}$ is the corresponding verification public key and $\mathcal{M}_i^{K}$ is the partnership's symmetric encryption key. P contains at least one such triple, composed of merchant's personal identifier and keys. Creation of the shared keys can either be performed by a designated server or by the participation of all the merchants [4].

Transaction records. A transaction record is a quadruple $(\mathcal{M}_i, m, c, \sigma)$, where $\mathcal{M}_i$ is the partnership identity under which the transaction is made (chosen by the merchant), m is the transaction encrypted with $\mathcal{M}_i^{K}$ so that the merchant and his partners only have access to the transactions made with the customer, not to other transactions, c is the transaction encrypted with $\mathcal{C}^{K}$ so that the loyalty device owner has access to all his transactions and σ is the signature of the transaction produced by $\mathcal{M}_i^{K_s}$ in order for merchants to authenticate the transaction. This signature also provides non repudiation and integrity of the transaction (non forgeability).

3.2 Procedures

In this section, we describe how a new transaction is stored in the loyalty card, how a loyalty program is executed so that a customer obtains an advantage and how a customer can check her transaction. For each procedure, we assume that the customer has to make an action (such as entering a PIN code or pressing the keypad of the reader) before each interaction with the merchant's terminal. This is a way to "authenticate" the customer and to prevent attacks such as denial of service.

Writing a new transaction. The recording protocol between the loyalty device and the merchant's terminal is sketched in Figure 1. When a customer makes a transaction $\mathcal{T}$ with a merchant $\mathcal{M}_i$, the merchant's terminal first requests the customer's pseudonym $\mathcal{C}^{\mathcal{M}_i}$ to the loyalty device by providing $\mathcal{M}_i$ to it. If necessary, the loyalty device generates a new pseudonym and records it. Upon reception of $\mathcal{C}^{\mathcal{M}_i}$, the terminal compiles the new transaction $t = (\mathcal{T}, \mathcal{C}^{\mathcal{M}_i}, \mathcal{M}_i, 0, \cdots)$, where "$\cdots$" denotes the additional transaction attributes, such as the amount of the transaction and the goods identifiers. The terminal then performs the following tasks:

1. Signs the transaction t using $\mathcal{M}_i^{K_s}$ to obtain σ.
2. Encrypts the transaction t and the signature σ using the chosen $\mathcal{M}_i^{K}$ to obtain m.
3. Authenticates himself with the loyalty card.

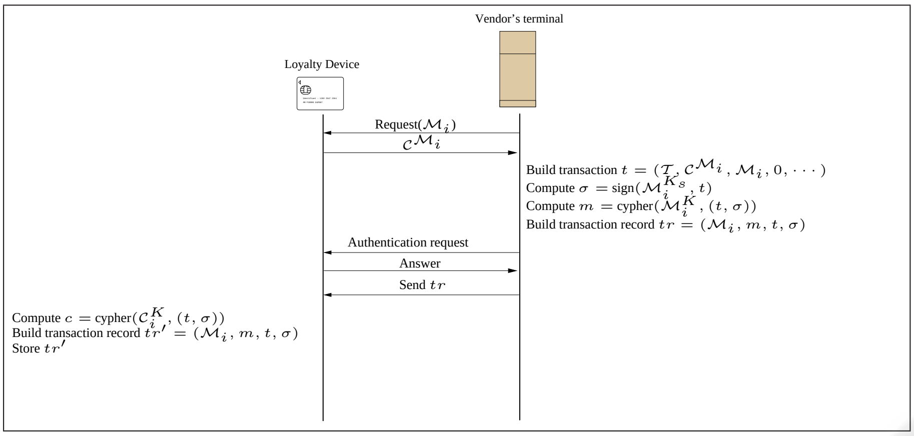
Vendor's terminal
Loyalty Device
Request($\mathcal{M}_i$)
$\mathcal{C}^{\mathcal{M}_i}$
Build transaction $t = (\mathcal{T}, \mathcal{C}^{\mathcal{M}_i}, \mathcal{M}_i, 0, \cdots)$
Compute $\sigma =$ sign($\mathcal{M}_i^{K_s}, t$)
Compute $m =$ cypher($\mathcal{M}_i^K, (t, \sigma)$)
Build transaction record $tr = (\mathcal{M}_i, m, t, \sigma)$
Authentication request
Answer
Send tr
Compute $c =$ cypher($\mathcal{C}_i^K, (t, \sigma)$)
Build transaction record $tr' = (\mathcal{M}_i, m, t, \sigma)$
Store tr'

Fig. 1. Recording a transaction.

4. Sends the transaction record $tr = (\mathcal{M}_i, m, t, \sigma)$ to the loyalty device.

Upon reception, the loyalty device encrypts transaction t and the signature σ using the customer's encryption key $\mathcal{C}^K$ to obtain c, and stores the resulting transaction record $tr' = (\mathcal{M}_i, m, c, \sigma)$. It should be noticed that the loyalty device records a transaction only if the transaction is indeed signed with one of the $\mathcal{M}_i^{K_s}$ keys. This prevents a terminal owner (*e.g.* a merchant acting as a customer) to use a terminal to copy past transactions on her own loyalty card in order to benefit from discounts illegitimately. In our system, we have chosen to add a merchant identifier in clear in each transaction record. This permits the loyalty program to only have the transaction that concerns the belonging merchant and, consequently, it does not have to treat all transactions in the loyalty device, but only the ones it is concerned with. This has the drawback of permitting a merchant to know the number of transactions the customer have performed with other merchants and potentially the identity of these merchants.

Awarding a discount. The awarding protocol between the loyalty program, the customer's device and the merchant is sketched in Figure 2. This protocol is independent of the merchant's loyalty strategy.

When requested by the terminal, the loyalty device returns transaction records whose merchant identifier field belongs to the set P of partnerships in which the merchant is involved. Each transaction is decrypted with the correct $\mathcal{M}_i^K$ and verified with the attached signature with the correct verification key $\mathcal{M}_i^{K_p}$. All transactions are then displayed to the merchant and the customer so that they can choose 1) which transactions will be used for the advantage and 2) which advantage[3]. The loyalty program then takes as input the above transactions, the description of the advantage and outputs the result of the advantage. The loyalty program sends the result to the merchant and optionally

[3] Depending on the strategy of the merchant, these choices can be made in cooperation with the customer or not.

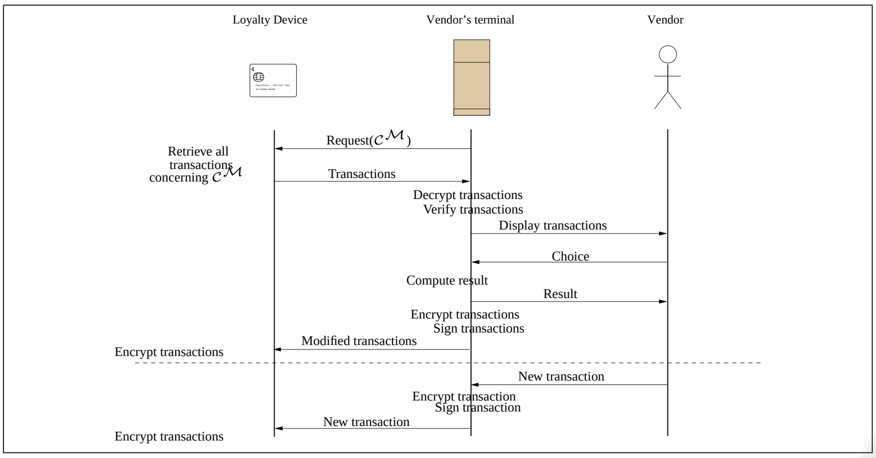

Fig. 2. Awarding a discount.

modifies all used transactions by updating their transaction counter s, depending on the loyalty strategy regarding multiple dipping. These transactions are then re-signed (using $\mathcal{M}_i^{K_s}$), re-encrypted (using $\mathcal{M}_i^{K}$) and sent back to the customer's device that re-encrypt itself the signed transaction (using $\mathcal{C}^K$). As for the storage of new transactions, the alteration of a transaction record is allowed only if the modified transaction is signed by the merchant's personal signature key.

Checking. A customer may check her transactions and advantages, assuming that she has access to a device reader. She first has to authenticate using *e.g.* a PIN code and the device then decrypts the transactions with the customer's decryption key $\mathcal{C}^K$.

4 Discussion

We now make a discussion of some problems and propose some solutions that we have not included in the global loyalty card system.

4.1 On the Privacy of Customers

In a way, this system provides a weak protection of identity, because external customer identifiers (*e.g.* a credit card number) might be used by merchants to link a customer identity with her personal data. Thus, as long as a customer uses a non-anonymous payment system, our system does not provide any practical gain in privacy. In fact, we simply assume that the merchant is honest and will not do anything else than recording information about the customer. Customer collusion is another problem. Multiple customers could collude to derive more benefits from sharing of a single system identity. This might be controlled if customers have to prove their identity when using their loyalty device, but would contradict our privacy-protecting objective. One solution for these problems is to use privacy protecting cryptographic tools such as the Direct Anonymous Attestations [3, 2] of the TPM (Trusted Plateform Module) or the TPD (Trusted Personal Device [6]) if we assume that the loyalty card can be protected by such modules. These tools also prevent the merchant to trace a customer, that is to link all transactions made by a particular user.

4.2 Preventing a Backup

In Section 2.4, we explain that a customer can fraud by backing up a list of transactions and copy them back on her loyalty card. We also said that a solution is to prevent the customer to write on her memory's device. This solution might be restrictive because it requires strong assumptions on the capabilities of the loyalty device. Another solution can be to add a merchant's identifier in clear in each transaction record and, for all transactions in which a merchant is involved and each time a transaction is added or modified, to have these transactions signed in only once by the concerned merchant. A MAC can be used here, instead of an asymmetric signature, to reduce the cost of this operation. Using this, the customer's device consequently contains a list of prints of all transactions that the customer has made with the same merchant. The case of a partnership does not imply any extra problem, a transaction being included in several prints.

4.3 Related Work

As much as we know, few papers have been published on the security side of loyalty cards. In [5], Enzmann *et al.* propose a privacy friendly loyalty system, which guarantees the unlinkability of loyalty points to transactions. One of the authors' objectives is to prevent vendors from generating customer profiles by linking customers' transactions through the loyalty program. The privacy protection side of our approach is not as restrictive, because it allows vendors to perform anonymous profiling. Patents have been proposed on loyalty solutions, but those claiming to bring security features mainly focus on the privacy issues. Several commercial solutions for loyalty system exist but it is unclear which security characteristics are proposed.

5 Conclusion

In this paper, we proposed an open and generic loyalty system based on smart cards which may be implemented in devices like ad-hoc smart cards or cell phones. The security properties of the system guarantee the security of the parties involved in loyalty strategies, *i.e.* that prevents dishonest customers and vendors from cheating and preserves users privacy. Our system presents some desirable features such as the possibility for customers to use one single loyalty card with any merchant, and for vendors to use a customized loyalty strategy, possibly in partnerships with other merchants. The features of the proposed loyalty system, together with the security properties allow to extend it to various fields of applications. For instance, customers can use the loyalty card as a reliable electronic receipt and estimates container with no modification.

References

1. National Institute of Standards and Technology. FIPS-197: Advanced Encryption Standard. November 2001.
2. F.C. Bormann, L. Manteau, A. Linke, J.C. Pailles, J. van Dijk. Concept for Trusted Personal Devices in a mobile & networked environment. 15th IST Mobile & Wireless Communication Summit, 2006.
3. E.F. Brickell, J. Camenisch, and L. Chen. Direct anonymous attestation. In V. Atluri, B. Pfitzmann, and P.D. McDaniel, editors, *ACM Conference on Computer and Communications Security*, pages 132–145. ACM, 2004.
4. R. Dutta and R. Barua. Overview of key agreement protocols. In *Cryptology ePrint Archive: Report 2005/289*, 2005.
5. M. Enzmann, M. Fischlin, and M. Schneider. A privacy-friendly loyalty system based on discrete logarithms over elliptic curves. In *Financial Cryptography*, pages 24–38, 2004.
6. IST-2002-507894, InspireD: Integrated secure platform for Trusted Personal Devices, http://www.inspiredproject.com.
7. RSA Laboratories. PKCS#1 v2.1: RSA Cryptography Standard. 2001.
8. W. Brian, and S. Seed. Making brand loyalty programs succeed. In *Journal of Brand Management*, pages 211–222, 2001.