uCard: A Novel Privacy Friendly Radio Frequency Tag Architecture for Universal Loyalty Card

Krishan Sabaragamu Koralalage and Noriaki Yoshiura

Department of Information and Computer Sciences,
Saitama University, Saitama, 338-8570, Japan
krishjp@gmail.com, yoshiura@fmx.ics.saitama-u.ac.jp

Abstract. According to some authoritative marketing analysis, a large percentage of daily sales are increased by its frequent customers. Due to the above fact almost all the stores started to implement point card or loyalty card schemes to achieve the eighty to twenty situation for both the customers and the retailers. Currently average customer has got at least five to six loyalty cards on different stores. Some venders have implemented such card system into the mobile phones. In addition to those cards each person at least has to have two or more hospital or access cards too. However subscribing several cards to achieve economical benefits have become a burden due to the difficulty arise when managing them. Therefore in this paper we proposed a novel privacy friendly loyalty card architecture which allows easy management of cards by using all-in-one card called uCard (Universal Card) using Radio Frequency Identification technology. Our universal card architecture will provide an ideal strategy for stores to build new relationships and to harvest the reward of customer loyalty by enhancing the customer experience while eliminating the hassle of managing several cards and decreasing the fear on personal privacy.

Keywords: Loyalty Card, Point Card, RFID.

1 Introduction

A loyalty card program is an incentive plan that allows any business to gather data about its customers. Customers are offered products or service discounts, coupons, points toward merchandise or some other reward in exchange for their voluntary participation in the program. A secondary goal of a loyalty card program is to build repeat business by offering participating customers something that isn't available to non-participating customers [2, 3, 4, 5].

Loyalty cards can be of several types: paper based cards, magnetic cards, smart cards, or software applet card in mobile phones. Typically a loyalty card has a barcode or magnetic stripe that's scanned at the point of sale. The card identifies the customer and sends information about what the customer bought to a database. The information in the database is used to help the retailer understand and influence his customers' buying habits [2, 3, 4, 5].

Nowadays, average customer has to have number of loyalty cards in their possession to use discounts on services or products. In addition to that most of them have to

L. Telesca et al. (Eds.): DigiBiz 2009, LNICST 21, pp. 53–63, 2009.

have several other cards such as hospital cards, insurance cards, credit cards, bus cards, train cards, electronic cash cards, etc too. Though holding several cards on various services or products help customers to receive efficient and discounted services or products, carrying bulky wallets with number of cards and picking the relevant card out of them has become a big burden.

Similarly some customers may have paper based cards, plastic cards or else card software embedded into a mobile phone. However, several forms of loyalty cards increase the complexity and also confuse the customers' day-today life. For instance imagine a situation where one customer has to manage four different personal identification numbers to manage four different loyalty cards in addition to bank cards and credit cards. It seems that the customers are already fed up with bunch of cards they have to keep in their wallets and remembering passwords and personal identification numbers as secret.

When investigated, we could find that it is always a unique number do these miracles. All most all the cards are identified uniquely by using a number or unique code. Only when the highly secured transaction is to be carried out, other properties are checked for verification. Otherwise all the data necessary to provide service or product are called from the proprietary database. Therefore the cards are used to locate the relevant record in service provider's database to provide better service.

One best option to solve the above mentioned problem is to make all-in-one card to use on any services or products. However, since the services and products wanted by one customer differ from others and the methods of such offering differ from provider to provider; there is no possibility to make one card with one unique identification number for all the services to use. Additionally some needs to be highly secured and some other needs no security at all [7].

Depending on the above requirements we came up with novel solution called uCard (universal card) to solve above problems. It is all-in-one card option but with secure role based accessing methods. It also enables the service provider to model their own number in uCard to compatible with their system. uCard has got secure communicational protocols to enable communications with any party securely [1, 6].

Rest of the sections in this paper is organized as follows. Section 2 describes the literature review. Section 3 describes the proposed solution uCard including its architecture and functionality. Communicational protocols are described in section 4 while the possibilities of uCard are discussed in Section 5. Finally section 5 concludes the paper with remarks and future works.

2 Related Works

There are many loyalty card schemes implemented in United States of America, Canada, Australia, Europe, Ireland, Germany, Switzerland, Hungary, Spain, Japan, Malaysia, Singapore, Indonesia, India, China, Taiwan and United Kingdom. Out of all the countries to the best of our knowledge there is no solution to relate with uCard other than Nectar in United Kingdom [2, 3]. The loyalty card market in the UK is one of the most significant in the world, with most major chains operating some form of reward system. Nectar loyalty card is one of the famous card schemes in U.K. and it was started by a partnership of suppliers including the supermarket chain Sainsbury's, the credit card American Express and the petrol distributors BP and initially launched in the autumn of 2002[2]. Sainsbury's, BP, Ford, EDF Energy, Expedia, Hertz, Brewers Fayre, Beefeater, American Express, TalkTalk, Dollond & Aitchison, The AA, Thomson Directories, Gala Bingo, Table Table, TNS mysurvey.com, Homebase are the members currently participating in Nectar loyalty card schemes[3].

Unfortunately, due to the security we are unable to know the architecture of the Nectar cards to compare with our proposal. However we believe that our solution is not similar to the Nectar in all the aspects other than the goal of providing all-in-one card to allow easy management for customers.

3 Proposed Solution: uCard

uCard is a universal card which can be used as a point card, loyalty card, club card, etc. Information stored in uCard is divided into two main parts: public information and private. Public information can be the information that needs no security or have less threat to personal privacy [7]. Private information need high security and can be used to store bank card, cash card, etc. uCard is a passive Radio Frequency (RF) IC chip which is designed according to the special requirements.

uCard can be of two forms. It can be used either as a plastic card or as a mobile phone by embedding a passive RF chip in it. If the same card system is to be used in computer communications, there must be a reader to take input from a plastic uCard or mobile phone uCard. Then uCard can be used as a web-card which will act like a loyalty card for the internet shopping or transactions. For simplicity in this paper we will describe the chip embedded plastic uCard. To be economical and secure, uCard should be made of UHF passive RF chip and restrict only a few millimeters of contactless reading distance. Depending on the demography and the country, expansion of the number of attributes and its division to public or private should be arranged. Normally forty to sixty divisions of public to private may be desired with possibility of expansion.

3.1 Conceptual Design of uCard

Using the object oriented concepts; uCard was designed to be encapsulated and allow access to its data only via its methods. Therefore uCard can be considered as an instance of an object class called Card. It has got public attributes, private attributes and methods to access those data. As shown in figure 1, uCard has got two methods: get method and set method. Figure 1 also illustrates the way uCard instance is generated.

Each uCard should consist of “oName=uCard” and “anonymousID=<random unique number>” at the time of fresh card generation. No private information can be accessed without approval of the card owner. Similarly no information including public attributes can be set without such approval. Following paragraphs describes the conceptual design and logical structure of the uCard. No personal information which can identify one individual person uniquely is included inside the chip. Instead the name and the expiration date may be printed on the card.

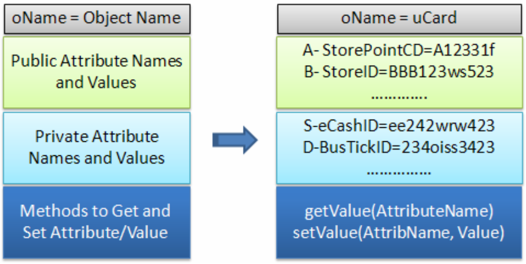
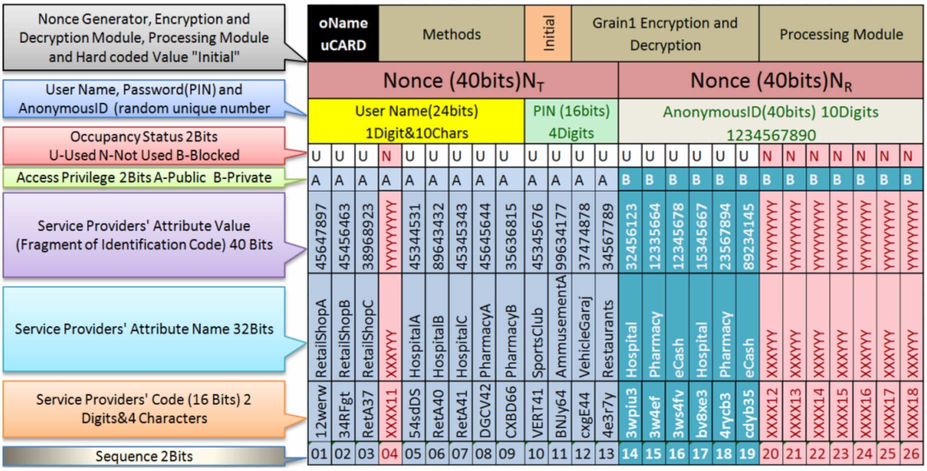


Fig. 1. Illustrate the instance definition of uCard

In uCard, role base accessing methods are implemented using access modifiers, memory types and encryption algorithms. Memory types used here are ROM, EPROM, and EEPROM. uCard controls writing permissions according to the access privileges. ROM is used for read only data and they are created by time of fresh tag manufacturing. EPROM is used for one time writing data and they are all about uCard information. EEPROM is used for all the rewritable data and those data can be changed any time on owner’s request.

3.2 Logical Structure of uCard

Figure 2 illustrates the sequence number, service providers’ code, attribute name, attribute value, access modifiers, occupancy status, user name, PIN and anonymous ID. Data belongs to a single row can be called an entity. Each entity includes sequence number, service providers’ code, attribute name and attribute value. An entity belongs to a one service provider. If someone needs to change an entity of retail shop P to retail shop Q, data belongs to entity P must be overwritten with Q’s entity after successful owner authentication process.


Nonce Generator, Encryption and Decryption Module, Processing Module and Hard coded Value "Initial"
User Name, Password(PIN) and AnonymousID (random unique number
Occupancy Status 2Bits U-Used N-Not Used B-Blocked
Access Privilege 2Bits A-Public B-Private
Service Providers' Attribute Value (Fragment of Identification Code) 40 Bits
Service Providers' Attribute Name 32Bits
Service Providers' Code (16 Bits) 2 Digits&4 Characters
Sequence 2Bits
oName uCARD
Methods
Initial
Grain1 Encryption and Decryption
Processing Module
Nonce (40bits)N_T
Nonce (40bits)N_R
User Name(24bits) 1Digit&10Chars
PIN (16bits) 4Digits
AnonymousID(40bits) 10Digits 1234567890

Sequence	Service Providers' Code	Service Providers' Attribute Name	Service Providers' Attribute Value	Access Privilege	Occupancy Status
01	12werw	RetailShopA	45647897	A	U
02	34RFgt	RetailShopB	45456463	A	U
03	RetA37	RetailShopC	38968923	A	U
04	XXXX11	XXXYYY	YYYYYYYYY	A	N
05	54sdDS	HospitalA	45344531	A	U
06	RetA40	HospitalB	89643432	A	U
07	RetA41	HospitalC	45345343	A	U
08	DGCV42	PharmacyA	45645644	A	U
09	CXBD66	PharmacyB	35636815	A	U
10	VERT41	SportsClub	45345676	A	U
11	BNJy64	AmmusementA	99634177	A	U
12	cxgE44	VehicleGaraj	37474878	A	U
13	4e3r7y	Restaurants	34567789	A	U
14	3wpiu3	Hospital	32456123	B	U
15	3w4ef	Pharmacy	12335664	B	U
16	3ws4fv	eCash	12345678	B	U
17	bv8xe3	Hospital	15345667	B	U
18	4rycb3	Pharmacy	23567894	B	U
19	cdyb35	eCash	89234145	B	U
20	XXXX12	XXXYYY	YYYYYYYYY	B	N
21	XXXX13	XXXYYY	YYYYYYYYY	B	N
22	XXXX14	XXXYYY	YYYYYYYYY	B	N
23	XXXX15	XXXYYY	YYYYYYYYY	B	N
24	XXXX16	XXXYYY	YYYYYYYYY	B	N
25	XXXX17	XXXYYY	YYYYYYYYY	B	N
26	XXXX18	XXXYYY	YYYYYYYYY	B	N

Fig. 2. Illustrate the logical structure of uCard RFID chip

Encryption algorithm used here is Grain1 stream cipher. Therefore encryption key size is fixed to 80 bits and it will be composed with anonymous ID, user name and PIN. Private information is transmitted after successful authentication with encryption. uCard contains methods, hard-coded data "Initial", Grain1 algorithm and processing module. uCard generates nonce N_I whereas the interrogator (reader/writer) generates three nonce values N_T, ID_I, and ID_T to carry out proper mutual authentication. Service providers' code is used to protect public readings. In addition to that, user name and PIN are used to ensure the security of both public and private writings.

Public and Private areas are marked as A and B respectively whereas occupancy status are marked as U, N, and B for used, not used and blocked. If three consecutive attempts are made retrieve same attribute value by sending wrong service provider code to the uCard, occupancy status will be changed to blocked status "B". After that, no data relevant to blocked card information row can be read until changing the occupancy status to "U". Similarly if wrong PIN is entered consecutively ten times the card will be blocked and have to bring it to the card management centre for recovery.

uCard is an all-in-one card and it is supposed to be filled with array of service providers' code, attribute name, and identification number. uCard do not store full identification number inside the tag, instead a fragment of the full identification number. The other fragment will be in the service providers' database system. Thus anybody without both parts of the identification number cannot try for any meaningful information from uCard. Additionally, it is not easy to gain access to service providers' database even if someone manage to read the fragment of an identification number stored inside the uCard. Hereafter fragment of identification number stored in uCard is referred as attribute value.

As explained in above paragraphs, information stored inside the card is categorized into public and private. In addition to that uCard has a built in authentication method to control read write permission. This has been achieved using a form of user name and password. Password here is considered as a PIN. For proper authentication it is necessary to pass the correct username and PIN to the uCard through the interrogator. Without proper authentication no writings are allowed to both public and private information. Similarly, the readings of private information need owners' authentication plus service providers' authentication whereas public attribute value can be read only with service providers' authentication. However, no service provider should be able to read the other information or other attribute name value pairs written in uCard even if the service provider is authenticated to read their attribute value. This is controlled by using the service provider code which act as a secret ID and stored inside the uCard. The service providers' code is not even known to the card owner but the service providers' database system. To read the each attribute value it is necessary to pass the sequence number, service provider's code and attribute name to the uCard. Then uCard check the validity of those inputs and send the desired results after validation and verification.

When reading public attribute values, there is no necessity to carry out owner's authentication process. Instead the attribute value will be issued only when the reader could pass the correct sequence number, service providers' code and attribute name to the uCard. Unlike public reading, in addition to above process; private reading, private writing and public writing need proper owner authentication before releasing or changing any information inside the card. Public modifier allows fast reading of any attribute value by any interrogator who has a common communication interface and could pass the correct sequence number, service provider code, and attribute name of attribute value to be read. The service providers' code will be different from subscriber to subscriber and even within the same service provider.

Private role is granted only to the owner of the uCard. He or she has the permission to read, write and overwrite any attribute name or value pair against the selected sequence number of the own uCard. However, card owner is restricted to read service providers' code written in own card. On the other hand, the owner has the right to overwrite any row of attribute value pair including service providers' code, if they are no longer wishes to use the some provider's services and needs to subscribe new service instead of current service. Even in new subscription, access to the new service providers' code is also restricted to the card owner. Sequence number in uCard is a fixed value and it is being built using ROM.

4 uCard Protocols

uCard has four main protocols: non-secure reading, secure reading, and secure writing and updating of user name and PIN. Protocol notations are as follows.

I	*- Interrogator (Reader/Writer)*
T	*- Tag (uCard)*
Kprv	*- Private Key [Anonymous ID, PIN, and User name] (80bits)*
PIN	*- Personal Identification Number [Password] (48bits)*
NI	*- Nonce generated by Interrogator (40bits)*
NT	*- Nonce generated by Tag (40bits)*
IDI	*-Interrogator generated ID (16bits)*
IDT	*- Interrogator Generated ID (16bits)*
Initial	*- Publicly defined initial message (16bits)*
R	*- Response value – Attribute Value, or Successful/Failed [1/0]*
{M}K	*- Message "M" encrypted by Key "K" using Grain1 steam cipher algorithm*

4.1 Non-secured (Public) Reading Protocol

Non-secure reading protocol is used for public reading. Any reader can query the public attribute values by passing the sequence number, service provider code, and attribute name to the uCard as shown in figure 3. For that it is necessary to identify the uCard instance first. To recognize the uCard instance, query is made to get the oName and anonymousID. If oName attribute value is of "uCard" then the service providers' interrogator asks to search its database to find the relevant sequence number, service provider code, and the attribute name to make the query to retrieve the desired attribute value stored in uCard. Once uCard receive a request from interrogator, received data will be matched against the own data and respond with the attribute value if three of them match with received values. In case if there is no match found inside the card, the block counter will be increased and failure will be informed to the interrogator. Likewise each time the mismatch occurs the block counter will be increased. If a proper match is found before the third consecutive wrong attempts, counter will be reset otherwise the occupancy status will be changed to "B" by blocking the readings of that particular entity until it is reset to "U". Once an entity is blocked, no access to the attributes of blocked entity can be made until the occupancy status is set to “U” with owner’s authentication by providing the user name and PIN. In the service providers’ side, once the attribute value is read successfully, interrogator composed the absolute attribute value by adding the service providers’ part into the retrieved attribute value and then locates the customer’s record to provide special services or facilities.

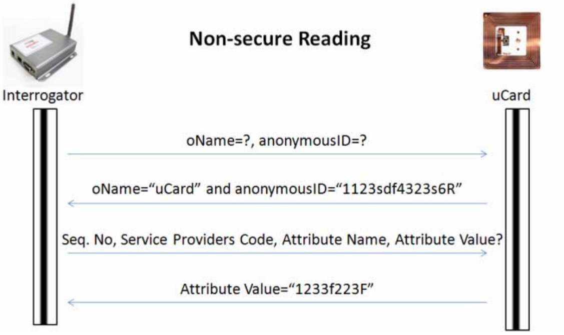

Non-secure Reading
Interrogator
uCard
oName=?, anonymousID=?
oName=“uCard” and anonymousID=“1123sdf4323s6R”
Seq. No, Service Providers Code, Attribute Name, Attribute Value?
Attribute Value=“1233f223F”

Fig. 3. Illustrate the public reading protocol

4.2 Secured Reading (Private Reading)

Unlike in non-secured reading, each attribute row must be managed securely. Reading is allowed only after successful mutual authentication. Here the KPRV denotes the Encryption key which is a combination of anonymous ID, user name and PIN. Like in non-secured reading, interrogator finds the relevant sequence number, service provider’s code and attribute name before querying the attribute value. Then those three values are passed to uCard, after proper owner authentication. Here the authentication is carried out by taking the user name and PIN as input to the desired reader. Hence only the service provider can read these attributes after receiving owner’s permission. Additionally, to ensure security of each reading messages are encrypted with encryption key and send as shown in Figure 4.

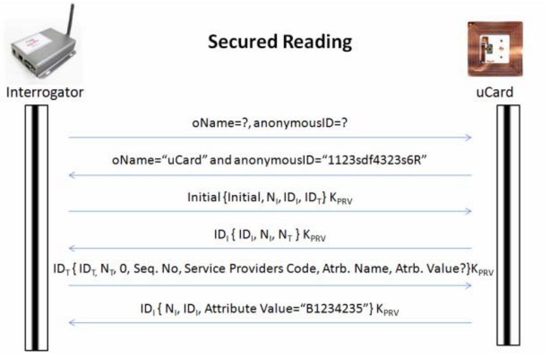

Secured Reading
Interrogator
uCard
oName=?, anonymousID=?
oName=“uCard” and anonymousID=“1123sdf4323s6R”
Initial {Initial, N_I, ID_I, ID_T} K_{PRV}
ID_I { ID_I, N_I, N_T } K_{PRV}
ID_T { ID_T, N_T, 0, Seq. No, Service Providers Code, Atrb. Name, Atrb. Value?}K_{PRV}
ID_I { N_I, ID_I, Attribute Value=“B1234235”} K_{PRV}

Fig. 4. Illustrate the secure reading protocol with private role key

4.3 Secure Writing

Same as in the secured reading, the secured writing needs successful mutual authentication. Attribute name and attribute value pair should be passed with the one of the service provider code selected from service providers' database. After successful writing, interrogator will be acknowledged with new sequence number, written service provider code and attribute value to confirm the information and enable the future readings as shown in Figure 5.

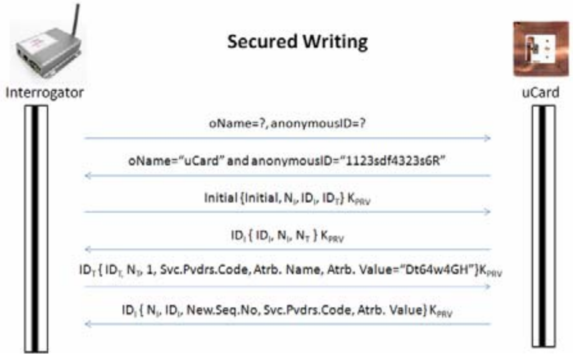

Secured Writing
Interrogator
uCard
oName=?, anonymousID=?
oName="uCard" and anonymousID="1123sdf4323s6R"
Initial {Initial, N_I, ID_I, ID_T} K_{PRV}
ID_I { ID_I, N_I, N_T } K_{PRV}
ID_T { ID_T, N_T, 1, Svc.Pvdrs.Code, Atrb. Name, Atrb. Value="Dt64w4GH"}K_{PRV}
ID_I { N_I, ID_I, New.Seq.No, Svc.Pvdrs.Code, Atrb. Value} K_{PRV}

Fig. 5. Illustrate the secured writing protocol with private role key

4.4 Updating User Name and PIN

Same as in the secured reading and writing, updating of user name and PIN can be carry out in uCard. Both of them cannot be updated simultaneously instead one by one. This process needs two more passes than secured writing since it is necessary to confirm before making the actual update. Once the confirmation is issued by the reader the encryption key will be changed to the K'_{PRV} by composing a new encryption key with changed user name or PIN as shown in figure 6.

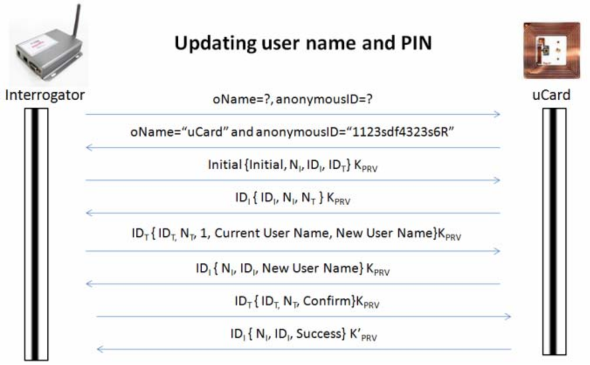

Updating user name and PIN
Interrogator
uCard
oName=?, anonymousID=?
oName="uCard" and anonymousID="1123sdf4323s6R"
Initial {Initial, N_I, ID_I, ID_T} K_{PRV}
ID_I { ID_I, N_I, N_T } K_{PRV}
ID_T { ID_T, N_T, 1, Current User Name, New User Name}K_{PRV}
ID_I { N_I, ID_I, New User Name} K_{PRV}
ID_T { ID_T, N_T, Confirm}K_{PRV}
ID_I { N_I, ID_I, Success} K'_{PRV}

Fig. 6. Illustrate the secured writing protocol with private role key

5 Possibilities of uCard

Figure 7 illustrates the interested actors in communicating with the uCard. uCard can store the entities of several interested service providers to ease the locating of own records. Inside the uCard, within the entity, each service provider can use their raw data, encrypted data or else use the anonymousID which is available from the time of creation.

Private cards may be for hospitals, pharmacies, banks, electronic cash, access control, bus or train, student enrollment, parking permit, prepaid phone cards etc whereas public Cards may be of TV cards, game cards, restaurant cards, sports club cards, retail store loyalty cards, membership cards, amusement cards, vending machine cards, temporary access cards, clothing cards, dry cleaning cards, air ticket cards, gasoline stand cards, etc.

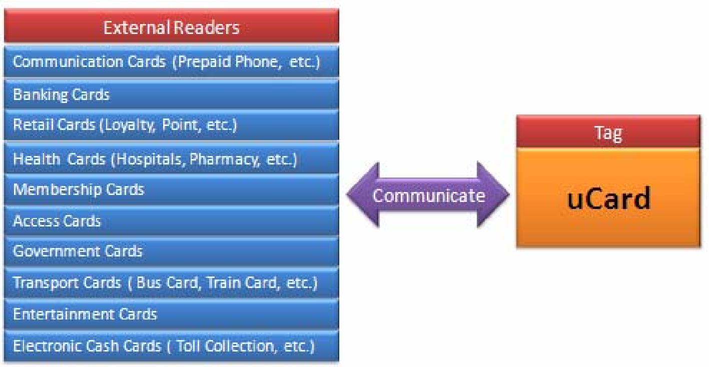

External Readers
Communication Cards (Prepaid Phone, etc.)
Banking Cards
Retail Cards (Loyalty, Point, etc.)
Health Cards (Hospitals, Pharmacy, etc.)
Membership Cards
Access Cards
Government Cards
Transport Cards (Bus Card, Train Card, etc.)
Entertainment Cards
Electronic Cash Cards (Toll Collection, etc.)
Communicate
Tag
uCard

Fig. 7. Illustrate the possible communicators of uCard

Initially the card should be issued by the city governing authority or through several selected retailers. It must be founded by the service providers and should be free of charge to users. Once the uCard is issued to a customer, it can be used for any compatible subscriptions. They may be from loyalty card to bank card.

Once the customer with uCard starts subscribing services, the entities of service providers can be set in the public or private area of the uCard depending on the customer's wish. For instance if one customer make any purchases from retail store P, the retail store P can suggest the customer to use a loyalty card option in their store. If the customer wishes to participate in their loyalty scheme, retail store's entity will be written to the uCard owned by that particular customer. Then the profile related to the entity written to the uCard of customers can be built into the service providers' database by implementing the loyalty scheme on him. Whenever the customer visit the retail store P, relevant entity of the uCard can be read and allow receiving special services provided to the subscribers.

uCard protect its security and privacy by storing absolute attribute value in distributed way. That is one part inside the card and the other in the service providers' database. Similarly the level of desired security can be managed in uCard by storing the information in public or private areas. On the other hand no public reading can be carry out without service providers' code whereas no private reading, private writing and public writing can be carry out without user name, PIN and service providers' code. Additionally, secure communicational protocols with encryption provides proper mutual authentication and there by guarantee the protection against the man in the middle and replay attacks. Furthermore, no repeated trials of entering wrong codes are allowed and no information belongs to other entities can be seen or retrieved by service providers even with proper authentication.

In case if uCard get corrupted, a new card can be issued from the card managing center and restore the old records after re-registering with service providers' system. When a customer loose the uCard or get it stolen, the card managing center must be informed immediately and their by issue a message to all the subscribers to suspends the transactions on lost or stolen uCard's anonymous ID. Then the risk on lost or stolen card can be alleviated. On the other hand, if attacker reverse engineers own or stolen uCard and receive the containing information, no big threat to service provider or customer occurs since the uniqueness of an entity depends on anonymous ID, sequence number, service providers' code, attribute name and attribute value. However there is a possibility to make several attacks with reverse engineered information though the risk can be reduced.

6 Concluding Remarks

Possibilities of using RF Chip with object oriented design to enhance loyalty programs efficiency are enormous; the only barrier is human imagination. uCard (Universal Card) which can be used to combine several cards to one card without creating any privacy or security issues is proposed. Further it provides the role base accessing and control in readings and writings. Finally the secured and non-secured protocols to communicate with uCard were also proposed. Since this is a feasible option, we are sure this solution will be workout in near future by creating a novel experience for customers and also for service providers by eliminating the hassle of managing several cards and decreasing the fear on personal privacy.

As future works, we are planning to improve this architecture to stand against the rest of the possible attacks, conduct formal verification on protocols, and extend the same system to embedded mobile phone card while enabling the web-card concepts in pervasive computing.

Acknowledgements

We would like to extend our sincere gratitude to Professor Takaomi Shigehara from the Department of Information and Computer Sciences in Saitama University on facilitating the environment for the above research.

References

1. Sabaragamu, K., Koralalage, Selim, M.R., Miura, J., Goto, Y., Cheng, J.: POP Method: An Approach to Enhance the Security and Privacy of RFID Systems Used in Product Lifecycle with an Anonymous Ownership Transferring Mechanism. In: Proc. SAC, pp. 270–275. ACM Press, New York (2007)

2. AIDC: Loyalty (Cards) Can Go Both Ways, Wednesday, February 18, 2009 - AIM Connections, http://www.aimglobal.org/members/news/
3. Nectar UK Loyalty Points Card, http://www.nectar.com/NectarHome.nectar
4. Loyalty program, http://en.wikipedia.org/wiki/Loyalty_program
5. Loyalty Schemes, http://www.moneysavingexpert.com/shopping/loyalty-scheme-tricks
6. Koralalage, K.S., Yoshiura, N.: OTag: Architecture to Represent Real World Objects in RF Tags to improve future Intelligent Transportation Systems. Journal of Convergence Information Technology 4(2) (June 2009)
7. Garfinkel, S., Juels, A., Pappu, R.: RFID Privacy: An Overview of Problems and Proposed Solutions. IEEE Security & Privacy, 34–43 (2005)