Security Extensions for Mobile Commerce Objects

Nazri Abdullah
Faculty of Computer Science and
Information Technology
Universiti Tun Hussien Onn Malaysia
Johor, Malaysia
anazri@uthm.edu.my

Ioannis Kounelis, Sead Muftic
School of Information and
Communication Technology
Royal Institute of Technology (KTH)
Stockholm, Sweden
{kounelis, sead}@kth.se

***Abstract* - Electronic commerce and its variance mobile commerce have tremendously increased their popularity in the last several years. As mobile devices have become the most popular mean to access and use the Internet, mobile commerce and its security are timely and very hot topics. Yet, today there is still no consistent model of various m–commerce applications and transactions, even less clear specification of their security. In order to address and solve those issues, in this paper, we first establish the concept of mobile commerce objects, an equivalent of virtual currencies, used for m–commerce transactions. We describe functionalities and unique characteristics of these objects; we follow with security requirements, and then offer some solutions – security extensions of these objects. All solutions are treated within the complete lifecycle of creation and use of the m–commerce objects.**

Keywords - mobile commerce; m–commerce; m-objects; security; privacy

I. INTRODUCTION

As mobile commerce (m-commerce) continues to evolve, it is a matter of time that it becomes the main source of online commerce [1]. In this paper, we describe our vision of m-commerce, by differentiating the goods that can be purchased in seven categories - we call them m-commerce objects. The m-objects have different requirements and are therefore treated in a separate way from the actors involved in a mobile commerce transaction.

We first provide the results of our analysis of the current concept of m-commerce objects. However, we also take two further steps: we consider the security features and the extensions that they need and moreover, what mechanisms and technology can be used to ensure and enforce such extensions.

Our research is focused on user aspects of various m–commerce systems, ensuring that the mechanisms we introduce allow users to protect their privacy and at the same time to verify authenticity, integrity and availability of digital goods that they are purchasing.

The next section of the paper describes various examples of m-commerce objects, based on our concept of a so-called generic m–commerce object. Section 3 introduces the main actors in an m-commerce scenario. Section 4 analyses security features and requirements targeted as goals of our design and also describes methodologies and technologies that can be used for implementation of those features. Section 5 demonstrates the dynamic use of the m-objects security features. Section 6 briefly introduces one of the popular m–commerce payment systems – Bitcoin and justifies our use of some of the innovative ideas that Bitcoin has introduced. Section 7 contains relevant work and compares the results with ours, while in section 8 we discuss our findings and approach. Finally, section 9 contains conclusions and suggestions for future work

II. SPECIFICATION OF MOBILE COMMERCE OBJECTS

It is important to understand the similarities and differences between various types of m-commerce objects. The definitions given below have been also documented in our previously published research paper [2]. The criterion for some well-known transactions to be classified as m–commerce objects is whether they have direct – explicit or indirect – implicit value. An example of an m–commerce object with explicit value is a pre–paid card – its value is money paid for the card. An example of an object with implicit value may be various discounts or benefits based on different types of memberships.

In this section, we list typical m–commerce objects described in some form of an order, starting from those that do not have explicit value all the way up to those that have strictly determined value. The objects are also "sorted" in the increasing complexity of their use.

The first type of m–commerce object is promotions. They publicize a product or a service with discount, so that the offered discount represents an implicit value of this type of m–commerce object [3]. In a mobile digital environment, these objects can be managed through personalized advertisements received through the Internet or even through a personal area network. A citizen with a Bluetooth enabled phone, for example, may receive personalized promotions or discounts to his/her phone via Bluetooth when shopping in a mall. The project PROMO demonstrates how this can be achieved [4]. Promotions do not require payments by users, which means that this type of m–commerce objects can be obtained without associated financial transaction.

The next type of m–commerce object is a mobile coupon. Those are text or picture vouchers solicited or purchased and delivered to a consumer's mobile phone. This object can be stored and exchanged for a financial discount, when purchasing a product or service [5]. The most important difference between promotions and coupons is that coupons have a value (expressed either as discount or monetary value), while promotions are mostly used for advertising of discounts.

The third type of m–commerce objects that we consider is a standard voucher used mainly today in paper form. It is a small printed piece of paper that represents the right to claim goods or services [6]. In the case of an m-voucher, there is no printed copy, but a digital equivalent with the unique identifier, such as a barcode or a Quick Respone (QR) code, stored locally on the phone or remotely at the m–commerce server. One example of such vouchers are coupons distributed by Groupon [7] or some other similar companies. In order to acquire a voucher, a payment transaction is usually involved. The difference between a voucher and a coupon is that the voucher is a complete representation of a product or a service, while the coupon is an offer/discount for the product or service. In other words, having a voucher means that the specific product has already been bought in advance while with a coupon consumers may claim it at alternative places or not at all, if the coupon was not purchased.

Another type m–commerce object is a gift card. In real life it is usually a tangible device (plastic card), embedded or encoded in a plastic, electronic or other form with a value based on a payment, which promises to provide to the bearer merchandise of value equal to the remaining balance of the card [8]. In a digital environment, a gift card can be seen as an equivalent to a very specific and limited pre–paid amount in an e-wallet, which can be used only with the specific merchant, in a particular shop or for a particular series of products. The difference with the voucher is that a gift card can be used as many times as possible, as long as there is credit left in the card. The voucher however is usually limited to one or to a predefined number of claims.

Mobile ticketing is an electronic realization with the help of a mobile device of the proof of access/usage of rights to a particular service [9]. There are many forms and ways to purchase a mobile ticket. Usually, a Short Message Service (SMS) message is the outcome of the purchase (the receipt).

A pre-paid card has many similarities with the gift card. It is a value stored in an e-wallet or in some account that can be loaded with money in order to be used mostly for micropayments [10]. The main difference with a gift card is that a pre-paid card is intended to be used by the owner and not to be gifted to another party and is usually not limited to specific merchants. More importantly, a pre-paid card can be recharged when the pre–paid amount is exhausted. By their purpose and type of transactions supported, the very popular pre–paid airtime may also be considered as one type of pre–paid card. In case of airtime, such m–commerce object is usually called telecom account.

Our final example and type of m–commerce object is a bonus card (also called loyalty card). This type of object usually refers to accumulation of points that a user gains from various purchases [11]. They are usually represented as supermarket cards, airline bonus cards, membership cards, etc., issued by merchants/businesses that give points to the customers depending on the value of goods or services that they previously purchased. Their owners can later use these points, in exchange for products or services. Such cards are usually free to acquire, but are bound to a user (or to a small closed and related group of users, such as members of a family).

III. The Concept Of M-Commerce Transactions

In this section, we introduce the main actors and define their roles in a typical m–commerce transaction together with the terms used and their interpretation. The purpose for the reader is to better understand the text in the remaining sections of the paper.

There are four actors in an m–commerce transaction:

1) *Merchant:* This is a business entity that offers some services or products for purchase. Merchants define availability, price, and all specific attributes of the m-commerce objects they issue and accept.
2) *Customer/User/Client:* The customer is the entity that obtains or purchases an m-commerce object in order to later redeem it.
3) *Redemption Point/Redeemer:* The place where m-commerce objects can be redeemed. In some cases this entity can be the same as the entity that issued the object, but most likely they will differ. For example, when buying a ticket for a concert, the merchant is the company selling tickets, while the redemption point is the venue where the concert takes place.
4) *m–Commerce Services Provider:* This is a trusted–third party in our system. It is the central entity that all other actors communicate with in order to handle their requests. Depending on the actor, different roles and services may be offered by the services provider. Merchants use the provider to make available their m-commerce objects, customers use it to acquire such objects and later use them, and redemption points use it for verification of validity of m-commerce objects in the redemption phase.

IV. Security Features And Attributes Of M-Commerce Objects

Each m-commerce object has a number of attributes that define it, both in terms of security and usability. Such attributes are required by both participating parties, object's issuers (merchants, m–commerce providers) and also by users, as their enforcement is an advantage for all parties.

A. *Authenticity of m–Commerce Objects*

This security property refers to the capability of the recipient to verify the originality of the m-commerce object, which includes verification of the identity of its issuer as well as correct and original contents of an objet. Verification can be performed by both the customer and the redeemer.

The customer should perform this check in the process of acquisition of an m-commerce object, i.e., before paying for it. This should be done in a timely manner, without interfering with the customer's purchasing experience in any way. In the best case, it should be an automated procedure, embedded in the acquisition phase and fully transparent to the user. The user should only be informed of the outcome of the procedure before giving the consent to proceed with the payment.

The redeemer should also perform verification of the object's authenticity before redeeming the m-commerce object. Such action should be performed with the assistance of the m–commerce Provider. This control will protect the redeemer against fraudulent attempts to acquire fake m-commerce objects.

Authenticity of m–commerce objects can be supported by the issuer (merchant or m–commerce provider) by digitally signing the object. Then the client will be able to verify the signature, as the certificates of either the provider or the merchant will be known to him/her.

B. *Security of m–Commerce Objects*

When referring to the security of an m-commerce object, we are actually referring to two different aspects: the *integrity* and the *confidentiality* of its content. These two issues together can be also interpreted as the user's privacy.

1) Integrity: Integrity refers to protection of the m-commerce object's values, against illegal intentional or accidental modifications, after its creation. This security feature is actually equivalent to the authenticity, described in the previous section. Therefore, all the mechanisms described above are also applied when referring to the integrity.

2) Confidentiality of Content/Privacy for the User:

Confidentiality of the content refers to the user's privacy when proving that he/she is the owner of an m-commerce object. This property is not applicable to all m-commerce objects, but rather depends on the type and also sensitive nature of the object.

Namely, the user should be able to prove that he/she is the owner of an object without revealing any information of what he/she has purchased with that object. The content of the object should be encrypted by the user upon purchase and will only be decrypted when redeemed. In the intermediate states, a header/part of the m-commerce object, indicating the owner, will be unencrypted, but signed by the issuer. If the m–commerce provider is involved, it is already in possession of user's identifying information and therefore there is no need to exchange any extra data with every purchase. The user should be able to define sensitivity level of the content in accordance to his/her preferences and then the system will enforce those preferences during the acquisition phase.

The security mechanisms for confidentiality of m–commerce objects are standard symmetric key crypto algorithms. What makes this feature very complicated to design and implement is use of partial values of some objects. For instance, gift cards or pre–paid cards may be partially redeemed. In such situations, encrypted objects must be decrypted, partially claimed, and then the new contents must be encrypted again.

C. *Duplication*

This is the property of m–commerce objects that specifies whether an object can be duplicated, i.e., whether a valid and legitimate copy of an m-commerce object can be created by its owner. Obviously, if objects have explicit value, this possibility should be prevented. In some virtual currency systems this feature is called prevention of "double spending".

In order to guarantee non–duplication, if required, a signature created over a random, unique, non–replicated value is needed. Therefore, the issuer will have to create a new value and sign a counter, possibly along with a timestamp, which when duplicated will not be possible to be changed, since in that case the signature will not be valid.

This security property is useful when an instance of an m-commerce object must be unique. For example, a voucher for a specific service or a ticket for a concert are examples of non–duplicated objects. On the other hand, if an m-commerce object is a free of charge promotion, it is actually in the merchant's interest to have the object duplicated and distributed as widely as possible, as this will give it more visibility.

The unique value or counter must be specified by the issuer in the process of creation of the object. In cases where users create copies of the object, the redemption of the second instance of the object will not be accepted as the unique value of the counter will be checked by the redemption point. This verification is very tricky in open, distributed environments and the Bitcoin concept has successfully addressed and eliminated this problem. This is one more reason why we have adopted its concept and some specific solutions for security of our m–commerce objects.

There is of course a risk that an m-commerce object is illegally duplicated after its first redemption and the illegal copy is distributed to some other entity. Then, when the legitimate owner tries to redeem the original object, he/she will be denied redemption. This problem may be eliminated by having the owner to sign the object as well. Therefore, if there is an attempt to redeem another copy of the same object, the owner will be consulted for approval as well. In addition, if the same person is trying to cheat the system, the unique identifier of the object will be sufficient to prohibit such action.

D. *Transferability*

This feature represents the property of an object to legitimately change ownership of an m-commerce object.

If objects are transferable, this action must be performed with the assistance of the m–commerce provider, since it is the actor responsible of signing the object and assigning its ownership. Moreover, even if a transfer is initiated or performed by one person to another person, the two entities will protect their privacy between them, as they will not have to exchange any details apart from their system identifiers (usually randomly assigned identifiers (IDs)).

The provider will receive a «transfer request» command from the current owner along with the ID of the recipient and then, if and only if the new owner meets all security requirements associated with the specific object, for instance age limit, the transfer will be performed. The owner of the object will be changed and the object will be re–signed by the m–commerce provider.

A drawback of this approach is the necessity to have provider's server connectivity at the time of the exchange. If the server is not accessible at the time of the transaction, the request may be temporarily saved on the current owner's station and when the connection is established, the request will be forwarded to the server and the transfer of the object will be performed.

Finally, in this stage of our research, the option to have a fee charged for this exchange is not considered. All transfers are free of charge. The payment in order to acquire the m-commerce object from the provider has already taken place from the first owner.

E. Monetary Value

Monetary value is the attribute representing the financial value of the m-commerce object, i.e., if it can be "exchanged" for something that has a cost.

This property does not provide any extra feature or option, as all the previous ones, but rather is a key factor affecting which of the previous mechanisms must be enforced to the specific m-commerce object itself. It can be better viewed as a property rather than an extra attribute.

If an m-commerce object has a monetary value, then, it is both in the merchant's as well as in the consumer's interest to have the object secured in all the above mentioned ways. As a conclusion, authenticity, non–duplication, integrity, and confidentiality for each object are needed.

The contents of each object are cryptographically encapsulated by the m–commerce provider and therefore the m–commerce objects cannot be tampered with. It is up to the object's owner to disclosure such information to any third parties or to reveal it only when absolutely needed (during the redemption process).

F. Purchased

M-commerce objects have this property if money is needed in order to acquire the object.

This property is strongly linked to the monetary value property. What applies there is also applicable to this property as well. The main difference whether an object has been purchased or not indicates solely the way in which the owner has acquired such object. Monetary value indicates also the actual value of the object.

G. Multiple/Partial Use

This property indicates whether an m-commerce object can be used more than once, i.e., if its total value may be partially redeemed. If yes, then such functionality can be enforced in two different ways:

1) There is a predefined number of uses that is decreased after each use (or increased when the user buys some more quantities of the object). An example may be tickets for public transportation.
2) It can be an amount (in Euros for example) that is decreased (or increased if the user charges the object). This is mostly valid for a gift card.

In both cases, the m–commerce provider must be involved in order to approve/confirm the remaining number of uses or the amount/value of the object. The new value of the object, after its adjustment, is signed and therefore can be verified by the provider at any time.

H. Tracking

This is the ability of the system to track past transactions and determine the current status of the object, i.e., the ability to track its full life cycle.

The attributes of the m–commerce objects that may be interesting when tracking are the date of creation, previous uses in terms of volume and content, and information about all previous owners. All these aspects depend on the type of the specific m-commerce object and the specific values of its attributes.

Tracking an object's history may be performed by the user without the need to engage the m–commerce provider in that process. For example, all previous uses can be recorded in the header of the object and in that way they may be retrieved in a read-only mode. They are always signed by the m–commerce provider. As such, it is generally recommended to reveal the values of all non–sensitive attributes (in terms of user privacy) in a read-only mode, so users can retrieve them at any given time and without requirement to be on-line, connected to Internet, in that process.

V. Dynamic Use Of Security Features

The security features described above are based on the basic set of security services: confidentiality, integrity and authenticity and may be applied during any phase of an m-commerce object's lifecycle. However, what makes these features different from the classical application of security services in some other network application is that they are applied in a very dynamic way.

The reason for the dynamic applicability is the complex reuse of the majority of the m-commerce objects. For example, a voucher that has a specific number of admissions to a service needs to have this number updated accordingly after each use. This implies that various features established in the initial phase when creating an object, are re-applied after every use of the object. Therefore, in case of m–commerce objects, special security protocols are needed, supporting repetitive application of security services. These protocols, therefore, effectively ensure that in all phases of its lifetime, each m-commerce object meets all the security requirements according to their special needs and properties.

As explained earlier, these needs and requirements are determined by the attributes of the specific m-commerce object, each depending on their contents and the nature of use. A full list of significant attributes for our m–commerce objects is given in Table 1.

TABLE I. M–COMMERCE OBJECTS AND THEIR ATTRIBUTES

	Voucher	Gift Card	Ticket	Promotions	Coupon	Bonus Card	Prepaid Card
Multiple Use	Maybe	Maybe	Maybe	Yes	Yes	Yes	Yes
Purchased	Yes	Yes	Yes	No	No	No	Yes
Monetary Value	Yes	Yes	Yes	No	Yes	Yes	Yes
Transferability	Yes	Yes	Maybe	Yes	Yes	No	Maybe
Duplication	No	No	No	Yes	No	No	No
Security	Yes	Yes	Yes	No	Maybe	Yes	Yes
Authentication	Yes	Yes	Yes	No	Maybe	Yes	Yes

The enforcement of security services that support those requirements takes place at both, the client side and the server side. Clients control object's authenticity and conformity to a predefined set of standard attribute values. The server creates these attributes and cryptographically encapsulates them, thus binding security credentials to the values of the m–commerce attributes. When a value of some attribute of an m-commerce object needs to be changed, the client sends a corresponding request to the server which performs the same procedure all over again, updating the values of m-commerce objects' attributes. By "client" in this case we do not necessarily mean the end–user but also any other entity in the m–commerce transactions chain, such as a merchant or a retailer. For a more comprehensive description of the actors and their interactions, the reader should refer to [2].

A. *Comparison with a traditional secure-by-design system.*

To illustrate how the dynamic nature of security services is different from some other traditional network applications, in this section, we compare our previous work of a secure e-mail system based on Secure/Multipurpose Internet Mail Extensions (S/MIME) and security proxies [12] and the dynamic use of security services described above.

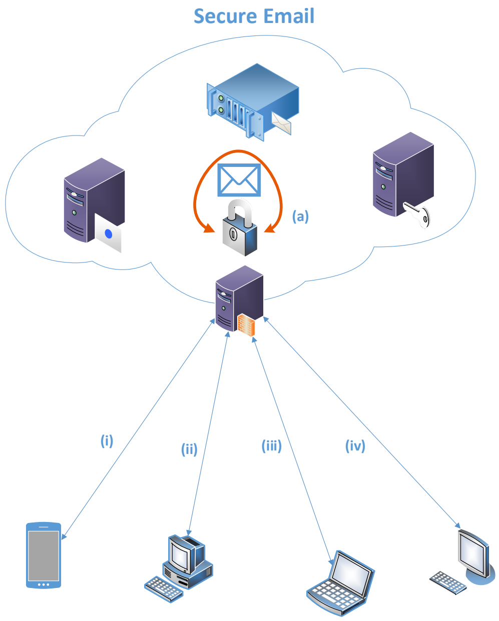

Figure 1. Secure Email Use. The security functionalities stay within the Secure Email proxy.

In the secure e-mail system, the use of security is straightforward. When a security method is applied, for example encryption or signing of an e-mail letter, a security action takes place at the e-mail client or at the security proxy and it is directly applied to the complete and final form of the specific e-mail letter. Then, in order to read such letter, i.e., decrypt or verify it, the e-mail client of the proxy server is again used. In the intermediate states of the protected e-mail letter, a third party cannot manipulate the message. For the client, the security is completely transparent; he/she only sees the "clear" output regardless of the way he/she accesses the proxy server. When accessing the secure e-mail from any end device (see Figure 1, i-iv), the result for the client is the same as for all the security functionalities that are performed internally.

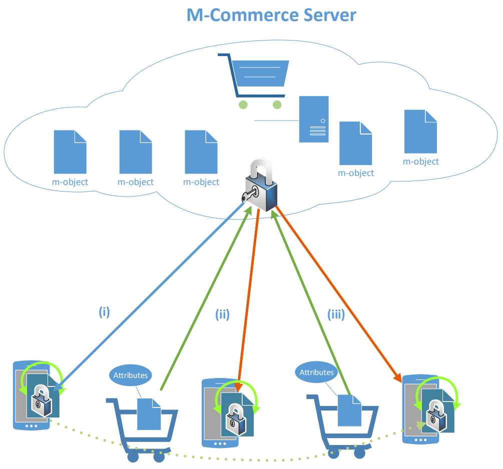

Figure 2. The dynamic reuse of security attributes for an m-commerce object.

In the m-commerce case, security services and mechanisms are re-applied after every use of the m-commerce object. Although there is a similarity in the two cases, in the sense that the server is the one that takes care of the enforcement of the security, the use for the client is different. When the client is using the m-object, the values of the m-object change. This directly implies that the signature and the authenticity of the m-object is not the same anymore and as a result the security attributes need to be readjusted to the new data. The server is the one that takes the responsibility of fulfilling this task and then resends the newly adjusted m-object to the client. The client, however, in this case has the ability to verify and recognize the security enhancements. This can be seen in Figure 2; as the m-commerce object is used in the real world (i-iii), its values change. These changes are taken into account each time at the server and as a result all the security attributes are re-applied. The attributes can be read not only by the server but also from the client side.

VI. Bitcoin System

Bitcoin [13] is a virtual currency that has become very popular in the last few years. It uses a peer-to-peer network to authorize and verify transactions and has no central authority like all other traditional payment systems. One of its main advantages is that the transactions are anonymous (actually pseudonymous) and third parties are not involved when performing payments or transfer of money, even for verification of participants.

Although the details of the protocol are not in the scope of this paper, we briefly review some of the innovative features that Bitcoin has introduced in the payment environment and we also indicate how these features can be applied and improved for security of our own system, that is for security of other virtual currencies.

The most interesting feature of the Bitcoin system is the concept and use of the blockchain. Transactions are grouped in specific blocks of data and these blocks are linked in the chain, called blockchain. Therefore, the blockchain contains and reveals the history of all transactions that have taken place in the Bitcoin system, since its creation. In order for a new transaction to be considered valid and accepted in the system, it must be included in the blockchain and then, applying mathematically and computationally complex procedures, be verified. Moreover, all accounts (Bitcoin addresses) in the Bitcoin system are publicly available, which means that anyone can check the balance of each account and how it has accumulated its current balance.

As Bitcoin addresses are long random strings of characters without any meaning and interpretation, there is no direct link between the owner of an address and the address itself. Nonetheless, it is still feasible for someone to try to find information that may be leaked about identities and the addresses that belong to them. This feature is also very useful in order to protect one's privacy. We would like to extend this feature by offering both anonymous transactions and by providing the possibility to have verified and authorized transactions for authorities and users who need verification of authenticity and reliability of selected transactions.

Our intention is to create a side-chain to Bitcoin, starting with one of the m-commerce objects. Side-chain is a separate blockchain, which is backed by Bitcoins, in the same way that currencies are backed by gold [14]. Doing so, we will be able to take advantage of the above-mentioned Bitcoin characteristics, while in the meantime manipulate the side-chain according to the m-object's needs.

VII. Related Work

The concept of m-commerce is not new to the research community. From the early years of mobile device adoption, both with the use of the first mobile smart phones or with the use of Personal Digital Assistants (PDA), the importance and potential growth of m-commerce was foreseen and a number of research solutions with a focus on security were proposed.

Nambiar et al [15] performed an analysis on payment transactions security in mobile commerce. As their research is 10 years old, technologies such as Wireless Application Protocol (WAP) and Java Micro Edition (J2ME) are not considered relative for modern development. Nonetheless, we consider the use of the SIM Application Toolkit still relevant, although still not used by major vendors, as demonstrated by our previous work [16]. Hughes [17] provides a comparison between Business-to-Business (B2B) and Business-to-Consumer (B2C), pointing out which Public Key Infrastructure (PKI) components are not necessary for a B2C marketplace. Lam et al [18] propose a lightweight security for mobile commerce transactions. Their proposal is based on public key cryptography and is end-to-end, thus avoiding any intermediate insecure actors. Chang et al [19] have proposed a secure e-coupon system for mobile users. The requirements Chang proposes are similar to ours with the difference that we extend them by including duplication, monetary value, multiple use and tracing.

We consider the above research results valuable input for our further research. However, it has to be pointed out, that as the works are relatively old, most of the restrictions mentioned are not applicable any more. For example, the computational power of the mobile devices, the wireless connectivity, the ease of use of modern smart phones and the powerful in terms of capabilities mobile operating systems, make it possible to overcome many of the restrictions that were mentioned a few years ago.

The most significant difference with our solution is that we propose a system that differentiates approach and security mechanisms depending on the nature of the m-object. The approach is not universal and applied blindly to all objects. That is the reason why we have distinguished and created the different m-object categories.

VIII. Discussion

In this work, we have presented and described our notion of mobile commerce objects, their use and special characteristics. We believe that the differentiation that we propose between these digital representations of goods is a useful distinction that could be a key enabler for future mobile commerce systems.

The most significant challenge we had to face was to clearly distinguish between the proposed categories of m-commerce objects. In fact, by searching the literature, the notions and terms used are some times mixed or may have a double meaning. For example, the difference between promotions and coupons is very delegate and may create confusion.

When dealing with a client-to-server connection, even more when the client is a mobile device, it is reasonable to face well-known vulnerabilities, specific to such environment. For example, threats like eavesdropping, spoofing, Denial of Service (DOS), data manipulation have to be dealt with when deploying such a system. We consider the description and further analysis of such threats not in the scope of this paper; we take however into account the results from [20] and [21] in order to deal with them in our future work.

Moreover, in order to avoid some of the human related vulnerabilities, e.g. having a mobile device stolen, we use secure storage of the m-objects on the user's device, as described in [16] and [22]. In such case, the m-object cannot be retrieved even in the case where the legitimate owner loses his/her device.

Finally, with the use of a mobile device as the main enabler of m-objects, it is evident that connectivity issues may appear. However, with the wide pervasiveness of wireless technologies, both mobile communications and Wi-Fi connections, we consider connectivity and speed connection to be less of a problem and not to influence the client experience.

Our goal with this article is to provide a reference for future use of m-commerce objects but to also propose what security and privacy characteristics are needed for them. With our distinction, we have made it easier to implement security enhancements for the m-objects as we provide guidelines on which requirements are needed. We also point out how this approach differs from a classical security solution from both the server and the client side. Our intention is to use the current paper as a reference for our further developments as described in the section below.

IX. Conclusions and Future Works

In this paper, we have described our concept of m-commerce objects and analyzed security mechanisms that are required in order to ensure protection and consistency of their attributes. We have also emphasized security services that ensure the integrity and authenticity of m-commerce objects. Those services are provided to all actors in the system, each having a different motivation and reason for ensuring the correctness of the objects and transactions. Moreover, we ensure customers' privacy by concealing sensitive information from intermediate parties. Finally, we refer to the Bitcoin system as a basis of the new paradigm for use of virtual currencies.

For future work, we plan to use some of the innovative mechanisms that Bitcoin has introduced for our design and implementation of the complex security system for the protection of virtual currencies. Anonymity and traceability of accounts and transactions are desired features in our design and implementation. However, they will be combined with the corresponding security enhancements that will allow legal entities to intervene in case of illegal transactions and activities.

References

[1] B. Siwicki, "E-commerce and m-commerce: The next five years," internetretailer.com, 28-Apr-2014. [Online]. Available: http://www.internetretailer.com/commentary/2014/04/28/e-commerce-and-m-commerce-next-five-years. [Retrieved: Oct-2014].

[2] I. Kounelis, G. Baldini, S. Muftic, and J. Loschner, "An Architecture for Secure m-Commerce Applications," in 2013 19th International Conference on Control Systems and Computer Science (CSCS), 2013, pp. 519–525.

[3] WordReference, "Promotion." [Online]. Available: www.wordreference.com/definition/promotion. [Retrieved: Jan-2012].

[4] PROMO, "Proximity Marketing Solution." [Online]. Available: http://isin.dti.supsi.ch/NetLab/index.php/promo. [Retrieved: Jan-2012].

[5] Mobile Marketing Association, "Introduction to Mobile Coupons," MMA, 2007.

[6] K. Fujimura and D. Eastlake, "RFC 3506 - Requirements and Design for Voucher Trading System (VTS)," 2003.

[7] "Groupon." [Online]. Available: http://www.groupon.com/. [Retrieved: Feb-2013].

[8] Kansas Statutes Annotated, "Unfair Trade And Consumer Protection: Consumer Protection," 2006.

[9] G. Me, "Security overview for m-payed virtual ticketing," in Personal, Indoor and Mobile Radio Communications, 2003, pp. 844–848.

[10] US General Services Administration, "Pre-paid Card," SmartPay. [Online]. Available: https://smartpay.gsa.gov/about-gsa-smartpay/glossary#p. [Retrieved: Feb-2012].

[11] Electronic Merchant Systems, "Loyalty Card." [Online]. Available: http://www.elect-mer.com/glossary-l.html. [Retrieved: Feb-2013].

[12] I. Kounelis, S. Muftic, and J. Loeschner, "Secure and Privacy-Enhanced E-Mail System Based on the Concept of Proxies," presented at the 37th International Convention on Information and Communication Technology, Electronics and Microelectronics - MIPRO, 2014, pp 1405-1410.

[13] "Bitcoin - Open source P2P money." [Online]. Available: https://bitcoin.org/en/. [Retrieved: May-2014].

[14] Z. Muadh, "Introduction To Sidechains and Blockchain 2.0," Deep Dot Web. [Online]. Available: http://www.deepdotweb.com/2014/06/26/sidechains-blockchain-2-0/. [Retrieved: Oct-2014].

[15] S. Nambiar, C.-T. Lu, and L. R. Liang, "Analysis of payment transaction security in mobile commerce," in Proceedings of the 2004 IEEE International Conference on Information Reuse and Integration, 2004. IRI 2004, 2004, pp. 475–480.

[16] I. Kounelis, H. Zhao, and S. Muftic, "Secure Middleware for Mobile Phones and UICC Applications," in Mobile Wireless Middleware, Operating Systems, and Applications, vol. 93, Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 143–152.

[17] J. Hughes, "Enabling E-Commerce Through PKI," Netw. Secur., vol. 2000, no. 3, Mar. 2000, pp. 14–16.

[18] K.-Y. Lam, S.-L. Chung, M. Gu, and J.-G. Sun, "Lightweight security for mobile commerce transactions," Comput. Commun., vol. 26, no. 18, Dec. 2003, pp. 2052–2060.

[19] C. C. Chang, C. C. Wu, and I. C. Lin, "A Secure E-coupon System for Mobile Users," Jan. 2006.

[20] D. Geneiatakis, I. Kounelis, J. Loeschner, I. N. Fovino, and P. Stirparo, "Security and Privacy in Mobile Cloud Under a Citizen's Perspective," in Cyber Security and Privacy, M. Felici, Ed. Springer Berlin Heidelberg, 2013, pp. 16–27.

[21] I. Kounelis, J. Loschner, D. Shaw, and S. Scheer, "Security of service requests for cloud based m-commerce," in 2012 Proceedings of the 35th International Convention MIPRO, 2012, pp. 1479 –1483.

[22] F. Zhang, I. Kounelis, and S. Muftic, “Generic, Secure and Modular (GSM) Methodology for Design and Implementation of Secure Mobile Applications,” presented at the SECURWARE 2012 , The Sixth International Conference on Emerging Security Information, Systems and Technologies, 2012, pp. 1–6.