SciForschen
Open HUB for Scientific Research

International Journal of Multimedia

Research article Volume: 1.1 Open Access

The Use of Policy Regulated Frameworks to Secure Mobile Commerce

Jan Löschner, Gianmarco Baldini*, Ioannis Kounelis and Ricardo Neisse

European Commission, Joint Research Centre (JRC), Ispra, Italy

***Corresponding author:** Gianmarco Baldini, European Commission, Joint Research Centre (JRC), Ispra, Italy, **E-mail:** gianmarco.baldini@jrc.ec.europa.eu

Received date: 29 May, 2015; **Accepted date:** 13 July, 2015; **Published date:** 17 July, 2015.

Citation: Löschner J, Baldini G, Kounelis I, Neisse R (2015) The Use of Policy Regulated Frameworks to Secure Mobile Commerce. Int J Multimed 1(1): doi: http://dx.doi.org/10.16966/ijm.101

Abstract

The evolution of mobile communication technology has fostered the development of new mobile multimedia applications in various domains. One of the most important applications is mobile commerce (m-commerce), which has an increasing impact in the life of the citizens, and could represent one of the many applications that contribute to the market success of the Internet of Things (IoT). Security and privacy concerns are quite relevant in m-commerce and IoT to protect financial and personal data of the citizens. One of the main issues in mobile commerce is how to ensure the security of the information needed to complete the m-commerce transaction in a distributed environment with different security frameworks. We have to consider that the protection of the m-commerce transactions must also be done to protect the privacy of the customer. In addition, the information of the m-commerce transaction can be fragmented in different files in a distributed m-commerce application, which can undermine the integrity (another security goal) of the transaction. In this article, we describe the design ofa m-commerce framework, where these issues are addressed through a policy based approach, where the access to the m-commerce transaction is regulated by policies. The fragmentation and integrity risks are addressed through the concept of Virtual Objects (VO), which have been defind in the FP7 iCore project. Policies are associated to VOs and distributed across the m-commerce applications. This paper describes the main concepts of VO and the policy based framework and shows how these concepts are applied to m-commerce in various scenarios to evaluate their feasibility. We apply and demonstrate the benefits of the proposed design to specific multimedia use cases of m-commerce where different domains are involved. Such as m-commerce system can be seen a basic underlying payment system for a wide variety of multimedia applications.

Keywords: Mobile commerce; Security; Privacy; Internet of things; Law enforcement

Introduction

The evolution of mobile communication technology has fostered the development of new mobile applications in various domains. One of the most important applications is mobile commerce (m-commerce), a subset of electronic commerce (e-commerce) that has an increasing impact on the life of the citizens and is seen as a powerful enabler by businesses to improve market effectiveness. Already in 2000, Varshney et al. [1] recognized the importance of m-commerce and defined a number of mobile applications, which have become successful from a business point of view in recent years. These applications include mobile payment, mobile entertainment services, mobile download of video or music, mobile procurements of products and services. In this specific article, we will focus on the mobile applications and related use cases of mobile payment as well as mobile procurements of products and services.

A more recent literature review on m-commerce is also provided [2], which identifies the main research areas to be further investigated. In particular, the authors point out the current fragmentation of architectural schemes and the lack of studies, which systematically describe the technical composition of main architectural alternatives and compare the main strengths and limitations of each. Another aspect highlighted [2] the need to guarantee security and privacy and the potential trade-off with usability: a complex security or privacy solution may be difficult to implement in the market and it may deter customers from adopting it, therefore disrupting the business case. More details on background work related to the topics discussed in this paper are provided in the Related Work section below.

The problem statement, we will try to solve in this paper include different elements, which are described in the following list:

1. Security and privacy concerns are quite relevant in m-commerce and many questions have been raised regarding mobile payments and virtual money. For example, coupons may require personal data of the consumers of the m-commerce applications. There is the need to design solutions, which do not hamper the effectiveness of m-commerce and also are able to protect the privacy of the users.
2. Because of the heterogeneity of applications, services and systems, which interact in a m-commerce scenario, there is a need to propose a common framework, which can be used to abstract and represent the assets to be searched and acquired (e.g., products), the users and the real-word objects, which participate to the m-commerce scenario (e.g., mobile terminal or a point of sale).
3. The organization and technological fragmentation of the m-commerce scenario can generate security vulnerabilities in the system because sensitive content related to an m-commerce transaction can be distributed in various components of the m-commerce scenario with different levels of trust. For example, the authors in [3] show the potential vulnerabilities in existing e-commerce systems, which accept payments through third-party cashiers.

To address these issues, this article proposes a framework based on the concept of encapsulation of digital information through Virtual Objects (VO), Composite Virtual Objects (CVO) and services, where the secure access and distribution of information is based on a sticky policy approach. The framework has been defined in the FP7 iCORE project [4]. In this article we describe the architecture of a secure and privacy enabled m-commerce system. We propose a framework that structures a m-commerce system in VOs/CVOs with semantic searching capabilities and an efficient and secure handling of system resources and transactions.

The objects (product, user data, vouchers, tickets, payment information) used in m-commerce are represented as VOs with the related list of attributes (e.g., type of product, merchant identifier).

In addition, the mobile terminals themselves can be represented as VOs and their features (e.g., processing power, bandwidth, presence of video camera) or dynamic information (e.g., location) can be represented as attributes of the VO and the collection and distribution of information can be tailored to the features of the mobile terminal.

The framework is based on the sticky policy approach proposed [5], where policies can be attached or "stick" to data to define allowed access rights and obligations as it travels across multiple parties or domains or mobile terminals, enabling users to improve control over their personal information. In our proposal the framework combines the concept of sticky policies with the concept of VO/CVO, which are created and managed with their associated policies and access rights to ensure data protection and privacy. We validate the proposed framework through the implementation and description of the workflow based on a voucher based use case. While security includes various functions: Availability, Confidentiality, Integrity, Authenticity, Non-repudiation and so on, in this article we will focus only on the Confidentiality of the data distributed in the m-commerce applications and how it relates to the authorization of the users to access resources.

The main objective is this article, is to show how the integration of well-known concepts (e.g., sticky policies, object oriented data encapsulation, semantic searching) can mitigate the challenges of heterogeneous applications and data in m-commerce scenarios and how the main actors can be represented in the framework.

The structure of the article is following: Related Work Section provides an overview of the related work. Mobile Commerce Section provides a description of the operational scenario for m-commerce, the related m-commerce objects and requirements. iCore Framework Section describes the architecture of the iCore framework and how the concept of sticky policies is applied. A Voucher Use Case and Workflow Section and e-Ticket Use Case and Workflow Section describe two use cases related to a voucher and an e-ticket. Comparison with Other Frameworks for Secure M-Commerce Section describes the implementation of the proposed framework for the use case described in Sections iCORE Framework and A Voucher Use Case and Workflow. Finally Conclusions and Future Developments Section concludes the article and describes future developments.

Related Work

The purpose of this section is to provide an overview of existing studies in m-commerce, which address the same or similar issues, which are identified in the previous section.

The importance of trust in m-commerce has been highlighted [6], which identifies the need to build customer trust but also underlines the complexity of the process both from a technological and business point of view. Consumers accessing and using m-commerce application face higher security and privacy risks because of the data transaction in a wireless environment and because of the nature of the distributed environment. The approach proposed in [6] is based on Analytic Network Process (ANP) from the Multi-Criteria Decision Making (MCDM) approaches and fuzzy logic from Artificial Intelligence (AI). By considering interrelationships among the trust factors, ANP is employed for selecting the appropriate website for mobile commerce. Another paper, which uses fuzzy logic in mobile commerce [3].

The identification of the main trust indixes in mobile commerce is proposed in [7]: (1) third party privacy seals, (2) privacy statements, (3) third party security seals, and (4) security features. A number of methods such as functionality, encryption devices, and digital signatures authorization can be usded to improve consumers' security in wireless communication and m-commerce. The proposed approach [7] is similar to what proposed in this paper even if the technologies are different, because our framework also tries to address the fragmentation of the m-commerce transaction in addition to the security aspects.

The customization and personalization of the user's profile is another important factor in m-commerce, which can also be addressed by the policy framework proposed in this paper. As described in [8], customization refers to the capability of a mobile site or a portal to modify itself or to be customized by users so as it is personalized to one's own needs and wants. Information regarding a user's mobile setting enables the automatic adaptation of the mobile interface and the potential content (e.g., products), which could be of interest to the customer. Customization reduces information load by filtering unnecessary information, thus alleviating the constraints of the limited visual display. The policy based framework proposed in our paper can also be used to support customization, because set of policies can be associated to the profile a single customer. While, the focus of our paper is more on the support for security and privacy, customization is a future development, which will be addressed by the authors in future papers.

A very recent paper on m-commerce is [9], which examines the evolution of the payment sector in financial services, specifically related to mobile payments (m-payments) for m-commerce. The main building blocks of m-commerce (i.e., technology components, technology-based services, and the technology-supported infrastructures) are analysed and discussed. The authors in [9] have indicated in the lack of security an important element, which can hamper the development and deployment of m-commerce applications. Single technologies (e.g., token) may not be enough to address all the security aspects of m-commerce or some technologies (e.g., QR code-based technology) can have limitations in m-commerce. As previously described, this is the major issue addressed in this paper.

Mobile Commerce

Figure 1 describes the mobile commerce (m-commerce) scenario with the relevant actors and domains including the iCore Framework. The m-commerce scenario involves the procurement and payment of products through ICT infrastructures and mobile devices. This scenario is characterized by different stakeholders.

The Merchant is the person that makes the goods (e.g, bottles of wine) or which can be reseller on behalf of the goods producers. The merchant inserts the information on goods in sale through an iCore web portal (i.e., part of the framework) or updates the existing information. The information is stored in the iCore repository as VO/CVOs with the access rights specified by the merchant or other factors (see the description of the government actors).

The Consumer is a person who is interested in using the iCore framework in order to acquire m-commerce objects (m-objects as defined in [10]). Such m-commerce objects can be vouchers, coupons, promotions, e-tickets, gift cards, etc. The consumer accesses iCore VO/CVOs through an iCore mobile application from his/her mobile device. For example, the consumer can acquire a voucher for a bottle of wine. In this article, the voucher represents the right to claim goods or services and it can be used once or to a predefined number of uses. It is usually associated to a discount on the good.

The Retailer is an entity that physically offers to consumers the products that are available at the iCore framework. The consumer can go to the retailer of his/her choice and redeem the voucher with the actual good. In some cases, the retailer is not an actual shop with a person but a service, like a vending machine for example.

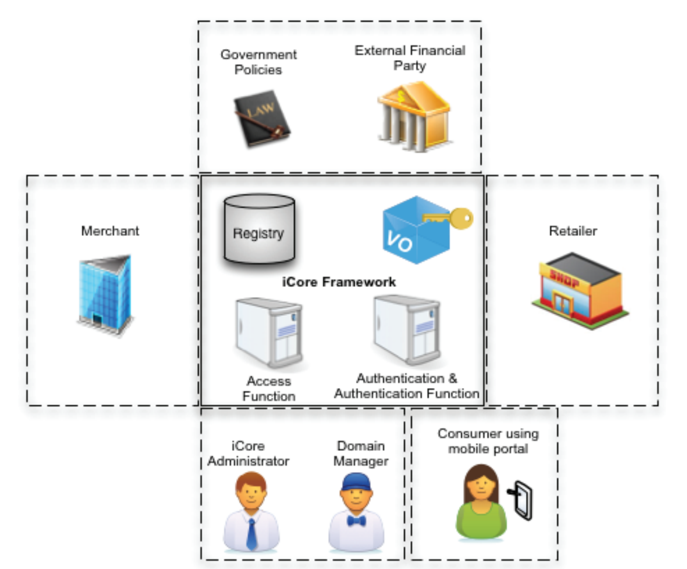

Figure 1: M-commerce application.

Besides the immediate users of the system, there are as well third parties that directly interact with the consumer, through the iCore framework, or interfere directly or indirectly with internal policies. Such entity is a third party financial party which handles all the payments. When a consumer needs to pay in order to purchase a voucher, the iCore framework will delegate the financial party to handle this payment. As a result, the consumer will choose to pay with his/her preferred payment to a party (s)he already trusts and iCore will not handle sensitive information, such as credit cards.

Another external party is the government or regulatory body which has a direct impact on the iCore policies. This actually refers to the laws that are applicable for each country. For example, when a consumer wants to buy a voucher for a bottle of wine, the regional law of age limit for alcohol consumption must be enforced. This enforcement can be automatically implemented by the iCore framework through access rights based on the attributes of the VO. For example, if a bottle of liquor has an alcoholic content higher than a certain amount, the level of access to liquor bottles should be granted only to adults over a certain age.

Finally, the domain of the iCore administrator includes the administrator functions. We can identify two main actors in this scenario. The Domain manager is responsible for inserting in the iCore framework information specific to the domains or can develop applications and logic targeted to the scenario. For example, the Domain manager specifies the levels of access related to the roles of the users (e.g., adult). Consider that we can have different domain managers for each domain. The other actor is the iCore administrator, which is responsible for the governance of the iCore framework.

In this scenario, each actor may be in different domains and different ICT infrastructures, but they all have access to the same iCore framework and related libraries. For example, the merchant introduces the information in an ICT infrastructure created for merchants, while the consumer can access an ICT application developed by a voucher provider. As a consequence, it is important to support secure distribution of information.

In this context we identify the following needed functions and mechanism:

- *Confidentiality* of the information created, distributed and stored in the m-commerce system, which can be composed by different domains and technologies. In some cases, the technologies and the networks cannot be fully trusted from a confidentiality point of view. As a consequence the proposed framework must protect the data even when it is transported over untrusted systems or networks.
- *Authenticity* of the m-commerce object refers to the user's ability to verify the originality of the m-commerce object the user purchases.
- *Privacy* of the user as the information provided by the user to complete the m-commerce transaction must not be disclosed to any unauthorized party.
- *Access rights* as the framework should provide the capability to regulate the access to the information stored in the m-commerce systems on the basis of the characteristics of the user.

iCore Framework

iCore architecture and components

The approach that we follow for this design derives from the FP7 iCore project [11]. The iCore project is dealing with the Internet of Things and has as a goal to mitigate the issue of heterogeneity between different objects and technologies while in the meantime maximizing the exploitation and provision of IoT objects. iCore is based on the principle that any real world object and any digital object that is available, accessible, observable or controllable can have a virtual representation called Virtual Object. A VO is primarily targeted to the abstraction of technological heterogeneity of the related real world object (e.g., a sensor) and includes a semantic description of the functionality. The iCore project proposes a framework where VOs can be aggregated in Composite Virtual Objects offering enhanced and more resilient services in accordance with the application requirements, which can support a service level. The structure of the iCore framework based on three levels (VO, CVO and Services) is described in Figure 2.

The iCore framework can be accessed at different levels and by different types of users. The iCore levels are used/created in a hierarchical structure, that means each overlying level uses services offered by the underlying level, but iCore also provides open interfaces to external business actors to each of the levels for direct access to the information as explained below.

Three main levels are identified:

1. Service level where users can access services provided by the iCore framework. The services can be generic or specific for a domain. The services can be composed and orchestrated to provide higher services. For example a service can be health monitoring of elderly patients in their house.

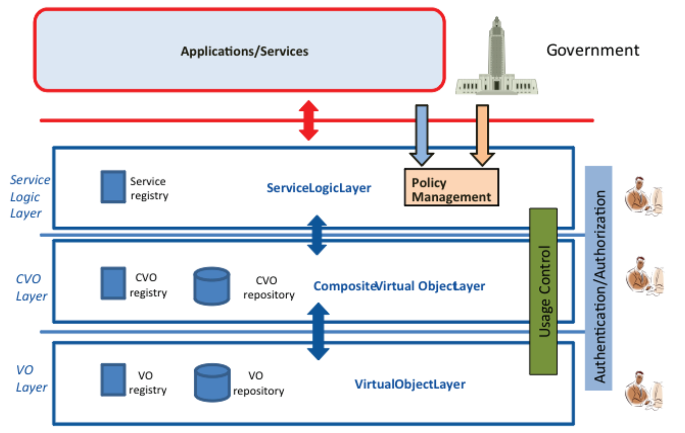

Figure 2: iCore architecture framework.

2. CVO level where users can search and retrieve information for a specific CVO. CVO is composed by VOs and additional so called service logic. For example, an insurance company can retrieve the data of a car.
3. VO level where users can search and retrieve information for a specific VO, which can be either a digital object or a proxy for a real world object.

Each level uses similar components for semantic searching, authentication, authorization and access to VO/CVO and services. These functions, which can be implemented as internal or system services in the iCore framework are:

- The *Registry* is the entity that has the responsibility of holding the references to the VOs/CVOs and the services available in the iCore framework. The registry provides the function of semantic search, which can be used by users and applications to identify the VOs/CVOs/services they need on the basis of the category and the attributes. The iCore registry is based on similar concepts to OWL-S described in [12] but it is extended to VOs and CVOs as well.
- The *Authentication and Authorization* block in the diagram includes both the authentication service and the authorization service. The design of the specific authentication service is out of scope of the iCore framework and any authentication mechanism (e.g., sign-on) can be used, but the identity of the authenticated user must be registered in the iCore framework. Note that a user can be either a person or an application. The Authorization service is linked to the Usage Control function as the user must be authorized to perform specific operations, which can be defined with an Access control mechanism.
- The *Usage Control* function regulates the access to VOs, CVOs and services. Depending on the level of access of the user, the access control function can allow or deny a transaction in the iCore framework (e.g., a m-commerce transaction). The role of the access control function is to store the mapping between role and access rights, grant access rights to VOs/CVOs and services and to maintain the association between the keys used in the sticky policies model (see next section) and the access rights.

Policy enforcement

In iCore we adopt an event-based usage control model to manage authorizations and obligations using enforcement mechanisms. Enforcement mechanisms follow an Event-Condition-Action (ECA) structure. When the event specified in the Event part of a mechanism is observed and the Condition part evaluates to true, the Action part is executed.

Events are signalled by Policy Enforcement Points (PEPs) distributed at multiple layers of the iCore framework. An event is signalled by PEPs whenever a usage control relevant activity is executed or is about to be executed in the framework. We support therefore two types of events: actual and tentative events. The objective of these two event types is to allow the specification of detective and preventive mechanisms. Detective mechanisms are ECA specifications that simply react to the actual events and execute additional actions in response to these events. Preventive mechanisms react to tentative events, before a usage control sensitive activity is executed in the system, and may allow, inhibit, modify, or delay this activity [13].

The Condition part of a mechanism may contain complex expressions combining propositional, temporal and cardinality operators. We also support reference to identity attributes and context information obtained at runtime to allow dynamic context-aware policy decision.

Mechanisms in the iCore framework are specified and communicated together with virtual objects using a similar concept to sticky policies [5]. The idea is that when the VO is created, a set of usage control mechanisms is attached to this object in an encrypted format in order to regulate future rights and duties of this object during its lifecycle. The usage control function in the iCore framework is capable of decrypting the attached mechanisms and evaluating these mechanisms at runtime to ensure the usage control policies are respected.

The Usage Control function regulates the access rights and duties of VOs, CVOs and services. Depending on the level of access of the user, the usage control function can allow, deny, modify, or delay the execution of an activity [4] in the iCore framework (e.g., a m-commerce transaction). In addition to controlling the execution of activities, the usage control function can trigger the execution of additional actions in order to enforce duties and regulate the compliance of the framework to security requirements derived from law enforcement issues and regulations. The role of the usage control function is to manage policies specified by means of enforcement mechanisms that govern the use of VOs/CVOs and services. The usage control function is also responsible for managing encryption keys used to protect the enforcement mechanisms in a similar way to sticky policies. The policy enforcement inside the iCore framework can be seen in Figure 2, along with the basic iCore components, and relevant iCore actors.

A Voucher Use Case and Workflow

Description of the voucher use case

In this use case, a merchant makes available on the iCore framework a number of vouchers for purchasing bottles of wine with a special price. The merchant is using a portal from his/her business computer to access the iCore framework over Internet. Once the vouchers are registered, an iCore user using the iCore application for mobile devices, searches for vouchers and in the end purchases the wine voucher. Finally the user that bought the voucher goes to a retailer that offers the product and uses his/her voucher in order to get the bottle of wine he/she had already paid for. The use case of a voucher has been chosen because it involves different type of entities in the m-commerce domain.

Voucher Scenario: creation of the voucher VO

The workflow of the scenario is presented in Figure 3. The merchant that wants to make a number of bottles of wine available on the iCore framework authenticates through the iCore framework using a dedicated web-portal. The authentication itself is not in the scope of this paper and as a result we consider it as a normal secure authentication process. Along with the authentication, the merchant receives the appropriate authorization according to his/her role.

After authenticating, the merchant requests the creation of the wine vouchers and indicate the voucher's attributes. Such attributes are time life of the voucher (i.e., how long the VO will be valid for), the amount of bottles of wine that are available under the specific conditions (i.e., number of available VOs), the price of the bottles of wine, in which store the consumer can collect the wine, the description of the wine and so on.

After the merchant specifies the desired attributes of the voucher, the VO creator function will contact the access control function in order to request the policies that are bound to the already specified attributes. Beyond the access rights imposed by the merchant, additional access rights can be applied by the iCore framework on the basis of policies required by the government or regulatory bodies. In this particular case where the voucher is for a bottle of wine, a policy will be enforced which only allows this voucher to be purchased by a person older than 18 years old.

The policies are defined and they are enforced by encrypting the VO

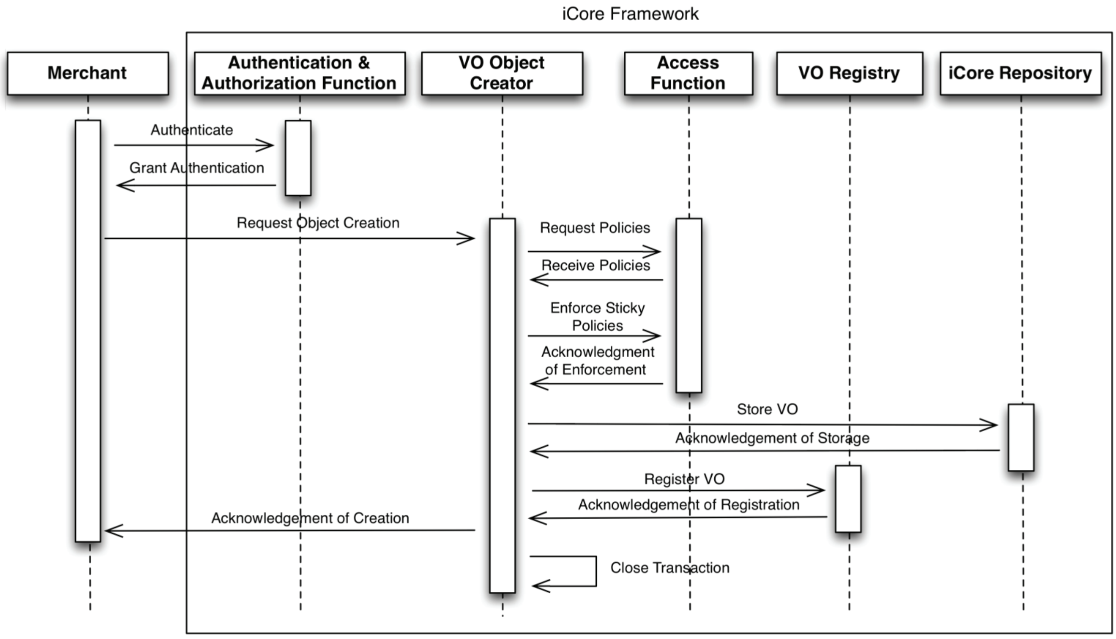

Figure 3: Creation of the VO voucher

with the keys corresponding to a specific level of access. The VO is then stored in the iCore Repository. After storing the VO, the Registry is updated. Thus, the registry contains a reference to the VO's actual location and in the mean time shows all its attributes. Finally, the merchant receives the positive feedback that the procedure was successful and the whole transaction is terminated.

Voucher Scenario: access to the voucher VO by the consumer

The workflow of the scenario is presented in Figure 4. A consumer is interested in buying a bottle of wine in a specific area (e.g., a town). The consumer uses the mobile phone and runs the iCore mobile application which connects to the iCore framework over the Internet. The consumer authenticates with his/her iCore credentials and then is logged in the system as a user.

The logic for executing a m-commerce transaction is implemented in a specific m-commerce service, which is implemented by the domain manager. Once connected to iCore, the consumer searches for a voucher with the desired criteria, when the voucher is found, the consumer proceeds with the purchase.

The m-commerce service forwards the request of the specific VO to the access server inside the iCore framework to ensure that this particular user is allowed to access the VO. Once access is granted, the attributes of the selected voucher from the VO registry are retrieved. Then the conformity of these attributes is checked. For example, it has to be checked that the voucher is still valid and has not expired, that there are enough items left to be purchased and also in this case if there are specific authentication needs on behalf of the consumer.

Once all the attributes are met, the payment needs to be performed. Payments are handled with a 3rd independent party, such as a bank. The access function will initiate the payment procedure at the 3rd party with all the necessary information. Then the user will be prompted to pay in the preferred way. Once the payment is successful, all the necessary attributes are met and thus the acquisition of the voucher can be completed.

At this point the m-commerce service can request access to the VO and retrieve the data needed for the consumer. A transaction wrapper is created in the execution environment by the m-commerce services and it is provided with the key related to the access level by the access function. In this particular implementation of the m-commerce service and the transaction wrapper, a new VO (i.e., VO voucher) in the repository is created containing the barcode, the consumer ID and all the possible retailers IDs from where the consumer can redeem his/her voucher. After receiving the acknowledgement, the registry is also informed about the new VO.

At this point the transaction wrapper sends back to the m-commerce service the barcode of the wine VO and all the retailer IDs. The m-commerce service forwards these to the consumer, which is now in possession of the barcode and transaction for the consumer is completed. Having all the retailers' information, the consumer can now choose where to redeem that voucher. In the iCore framework, the m-commerce service updates the wine VO's attributes in the iCore Repository and as well in the Registry. The changes indicate that the voucher has now been sold and is not more available for purchase. The final procedure in the system is to destroy the transaction wrapper and then terminate the transaction.

Voucher Scenario: retrieve the physical item at the retailer

This final phase describes the workflow for the retrieval of the physical item (e.g., bottle of wine) at the retailer place (Figure 5). The consumer, having in possession the barcode goes to one of the available retailers (already sent to the consumer during the purchase) and wants to redeem the voucher and get the bottle of wine.

The retailer is in principle already authenticated to the iCore framework and is given the corresponding role. The consumer shows the barcode to the retailer simply by showing it on his/her device. The retailer then scans the barcode and sends it to the m-commerce service. The m-commerce service acts in this case exactly as in the case of the consumer; it is the interface for the retailer in order to access the iCore framework.

At this stage, the validity of the barcode is checked. The registry is searched for the VO Product (each VO has the iCore id in clear even if the VO itself is encrypted) and confirms the originality and validity of the consumer request.

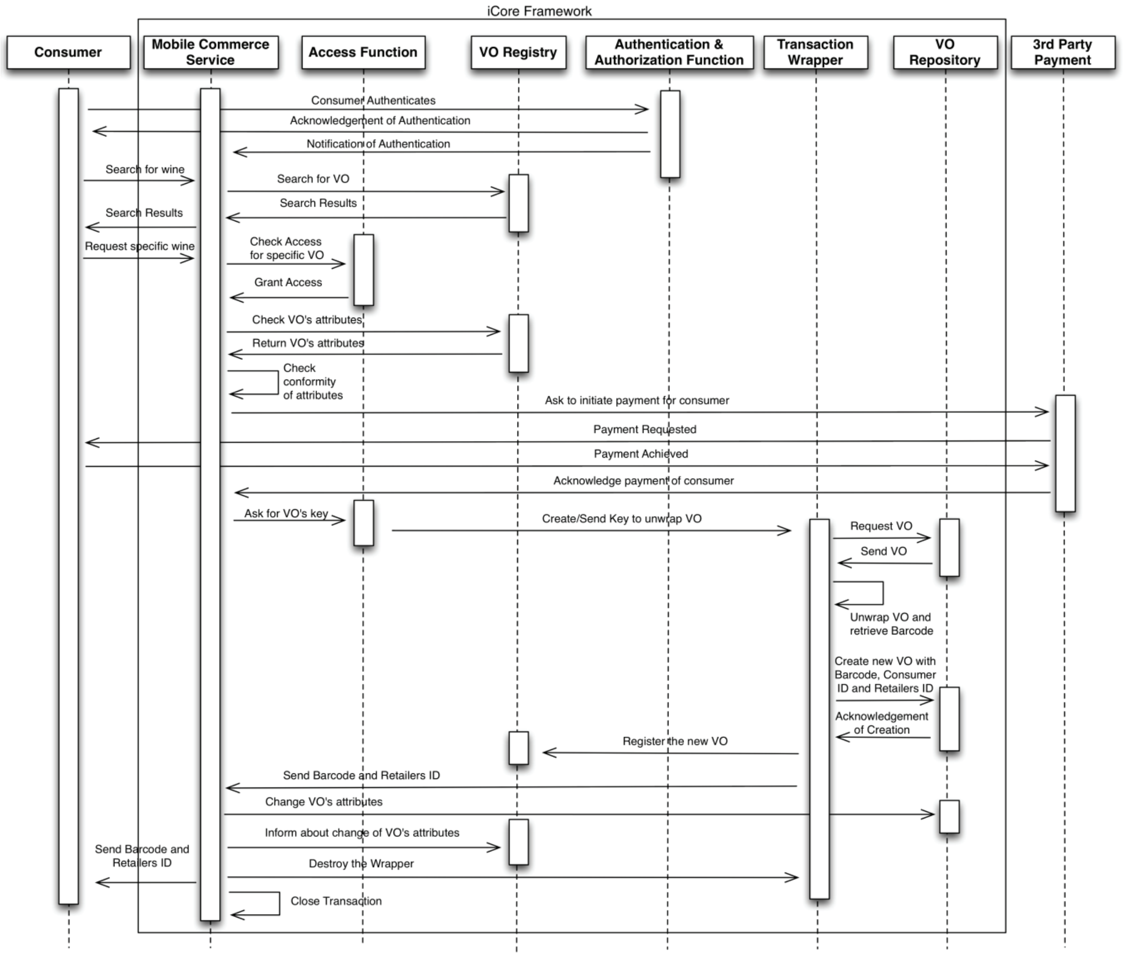
iCore Framework
Consumer
Mobile Commerce Service
Access Function
VO Registry
Authentication & Authorization Function
Transaction Wrapper
VO Repository
3rd Party Payment
Consumer Authenticates
Acknowledgement of Authentication
Notification of Authentication
Search for wine
Search for VO
Search Results
Search Results
Request specific wine
Check Access for specific VO
Grant Access
Check VO's attributes
Return VO's attributes
Check conformity of attributes
Ask to initiate payment for consumer
Payment Requested
Payment Achieved
Acknowledge payment of consumer
Ask for VO's key
Create/Send Key to unwrap VO
Request VO
Send VO
Unwrap VO and retrieve Barcode
Create new VO with Barcode, Consumer ID and Retailers ID
Acknowledgement of Creation
Register the new VO
Send Barcode and Retailers ID
Change VO's attributes
Inform about change of VO's attributes
Send Barcode and Retailers ID
Destroy the Wrapper
Close Transaction

Figure 4: Consumer access to the VO voucher.

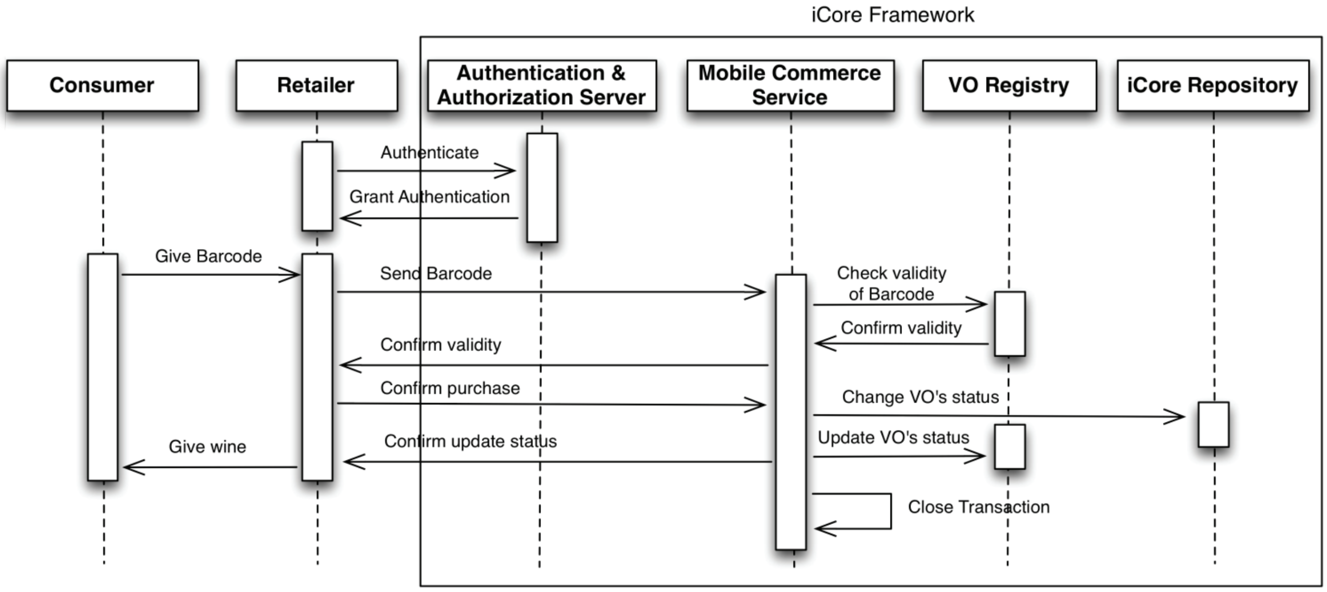

Figure 5: Voucher Scenario: retrieve the physical item at the retailer.

Citation: Löschner J, Baldini G, Kounelis I, Neisse R (2015) The Use of Policy Regulated Frameworks to Secure Mobile Commerce. Int J Multimed 1(1): doi: http://dx.doi.org/10.16966/ijm.101

Once the retailer receives the confirmation, s(he) can proceed with the transaction and handle the bottle of wine to the consumer. Then the retailer will need to inform the iCore framework of the successful interaction. The iCore Repository will have to be updated with the new VO attributes, indicating that the VO has now been redeemed by the consumer. After updating the repository, the registry will also have to be updated accordingly. Finally the whole transaction will terminate. The VO Product can be deleted or flagged for successful m-commerce transaction.

This scenario could also be achieved with a non-human retailer. For example, there could be a vending machine that has a barcode reader and then, upon receiving the barcode, performs the same tasks at described above.

In this case, the iCore VO container in the iCore execution environment described in [4] is used to interface the vending machine, both as a sensor function to read the barcode and the driving license of the consumer and as an actuator to provide the bottle of wine. The driving license of a similar ID card is used to identify the customer when specific authentication attributes are needed.

In another variation of this use case, the consumer could store on mobile devices (e.g., a smartphone) the VO Product itself as an encrypted object. Then the consumer could simply provide the VO Product to the vending machine to complete the transaction.

In all these use cases, the consumer, retailer and the merchant can all interface difference ICT infrastructures and domains furnished with the iCore framework. The VO registry is fully distributed among the different instances, but VOs can be securely moved or copied across untrusted domains or connections because they are encrypted. Figure 6 describes more in detail the inter-domain transaction between the retailer and the consumer domains. The picture is also based on the sticky policies concept described in [5] with the iCore access control function, which includes the function of Trust Authority [5].

The systemic functions of iCore represented by the VO registry and the access control function are distributed across domains and they are connected through trusted channels. The VO can instead be transmitted through untrusted communication channels or they can be stored in untrusted domains like a mobile phone, which is not equipped with an iCore interface. Once the VO is received by a user (e.g., the vending machine), the VO registry will provide the level of access to the VO and the access control function the correspondent key to get access to the VO data through a transaction wrapper.

Finally, it should be pointed out that the last step towards the user (delivery of product, confirmation of creation or receiving the barcode) happens only after the iCore system is updated correspondingly. This procedure is necessary in order to avoid situations where a malicious user can take advantage of a logic flaw and trick the system.

e-Ticket Use Case and Workflow

In order to illustrate the workflow and internal operations of the iCore framework in regards to the policy enforcement, we describe another case of an m-ticket use. We use complex, but nonetheless real-life scenarios, in order to demonstrate how different challenges are dealt with, how pseudonyms are used, how CVOs work, how delegation from a user to another is performed, how policy enforcement is applied and finally how law enforcements can search for illegal activities, while in the meantime protecting the citizens' privacy.

Description of the e-Ticket use case

An iCore user wants to buy a ticket for a football match from his/her mobile device. Moreover, he/she would like in parallel to make his/her travel arrangements to the stadium and, as a result, combines the stadium ticket with a train ticket. Finally, the user also buys a voucher for a beer, which he/she can pick up at the stadium's bar. The tickets and the voucher are different VOs, combined together in a CVO.

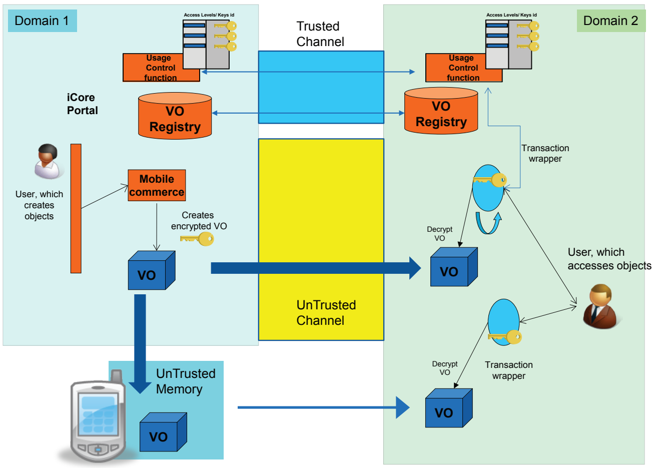

Figure 6: Sticky policies and distributed domains.

In our scenario, it turns out that the user will not be able to attend the football match, so he/she decides to give the stadium ticket, the train ticket and the beer voucher to a friend. In iCore, this transaction is seen as a delegation from one user to another to use the CVO he/she had already purchased. In order to perform the delegation, both users need to be connected to the iCore framework, in order to update the CVOs details in the registry. However, the actual transfer of the CVO between the users can be done directly from one mobile device to another, using Bluetooth for example.

The inspector is also an iCore user, with different access rights. When given a VO, he verifies the unique code by searching for it in the iCore registry and seeing the status of the VO. Upon the correct verification, the VO has its status changed, both in the iCore registry and in the user's mobile device.

In order for a user to use the iCore framework, (s)he will have to be registered first. As a result, all the transactions and purchases done under the same identity, can lead to having the user profiled and his/her privacy compromised. In order to avoid this and to implement privacy-by-design, we have introduced the use of pseudonyms [11], where a user has one pseudonym per context, making it difficult to link different identifiers across service contexts.

A pseudonym is a subset of the user's true identity that only reveals the absolutely necessary information, needed for a transaction to be completed. Moreover, attributes that are considered personal or sensitive, like age, are only partially revealed, as indicated in the project ABC4Trust [14] and decoupled from the real identity. The pseudonym reveals in our case only that the user is an adult, without giving his/her true age. Finally, the pseudonym cannot be linked back to the real user by a third party, and even in the case of a security breach, the access to the user's identity would be harder to reach.

An example of pseudonym for the above use case would be a pseudonym that is used when purchasing tickets for concerts or events in general. In such case the pseudonym identity would also reveal that the user is an adult, in order to be able to proceed with purchase of the beer. Other attributes that the pseudonym can have, would be seat preference at the venue, special ticket category (e.g., student, disabled), payment method, etc.

Citation: Löschner J, Baldini G, Kounelis I, Neisse R (2015) The Use of Policy Regulated Frameworks to Secure Mobile Commerce. Int J Multimed 1(1): doi: http://dx.doi.org/10.16966/ijm.101

Analysis of the internal workflow

In order to better demonstrate the workflow inside the iCore framework when events are triggered and specific policies need to be enforced, we have created two UML diagrams (Figure 7). It must be pointed out that the diagrams do not include all the transactions and interactions between the iCore framework components, but only the ones that are relevant and necessary to describe the policy enforcement part.

Automatic enforcement of a predefined policy

The first diagram, in Figure 7, presents the case where an event triggers a predefined policy, which is then automatically enforced. In particular the delegation of the CVO, as described in the previous sub-section, cannot be fully completed due to the age limitation of the consumer B. In order for the user to buy a beer, (s)he should be above the national allowed age limit. This policy is not only performed during the purchase of the beer coupon, but also during the transfer from one user to another. As a result, if the second user does not meet the age requirement, (s)he would be still able to receive the other two VOs (stadium and train ticket), but the VO linked to the beer will stay with the original user.

The workflow is the following:

- Both users need to be connected to the iCore framework. This connection is achieved through the corresponding interface, here named m-commerce service.
- After being connected, user A delegates user B to use the CVO. The delegation is performed using a Bluetooth connection, without the use of the iCore framework. However, after the local delegation, both users contact the iCore framework in order to confirm and register it.
- The m-commerce service receives both requests and proceeds with the change of the CVO owner. The first step is to inform the registry (in particular the CVO registry) of the user change.
- The PEP is triggered by this event (change of owner) and performs checks in case a specific policy will need to be enforced. The check is performed in each VO independently.
- When the check arrives at the beer voucher, the age policy needs to be enforced. As a result the PEP informs the PDP of this activity. The PDP will then check with the registry if user B meets the required age limit.
- The registry responds to the PDP that the user does not meet the age requirement and as a result the PDP denies the delegation of the specific VO to user B. This VO will not change status and will have user A as owner.
- The registry performs all the modifications and informs the m-commerce service. The former informs both users on the delegation status and as a result they can also see the representation of the VOs locally on their mobile device.

Detection of a suspicious event

The iCore framework enables the monitoring of transactions, in search of various search patterns, that may result in criminal activities. For example, in our scenario it may be of the authorities' interest to observe users that decide to delegate the ticket of an anticipated football match only a few hours or minutes before the start of the match, as this may be an act of black market transaction. However, it must be pointed out that the monitoring of the transactions is done without knowing the identity of

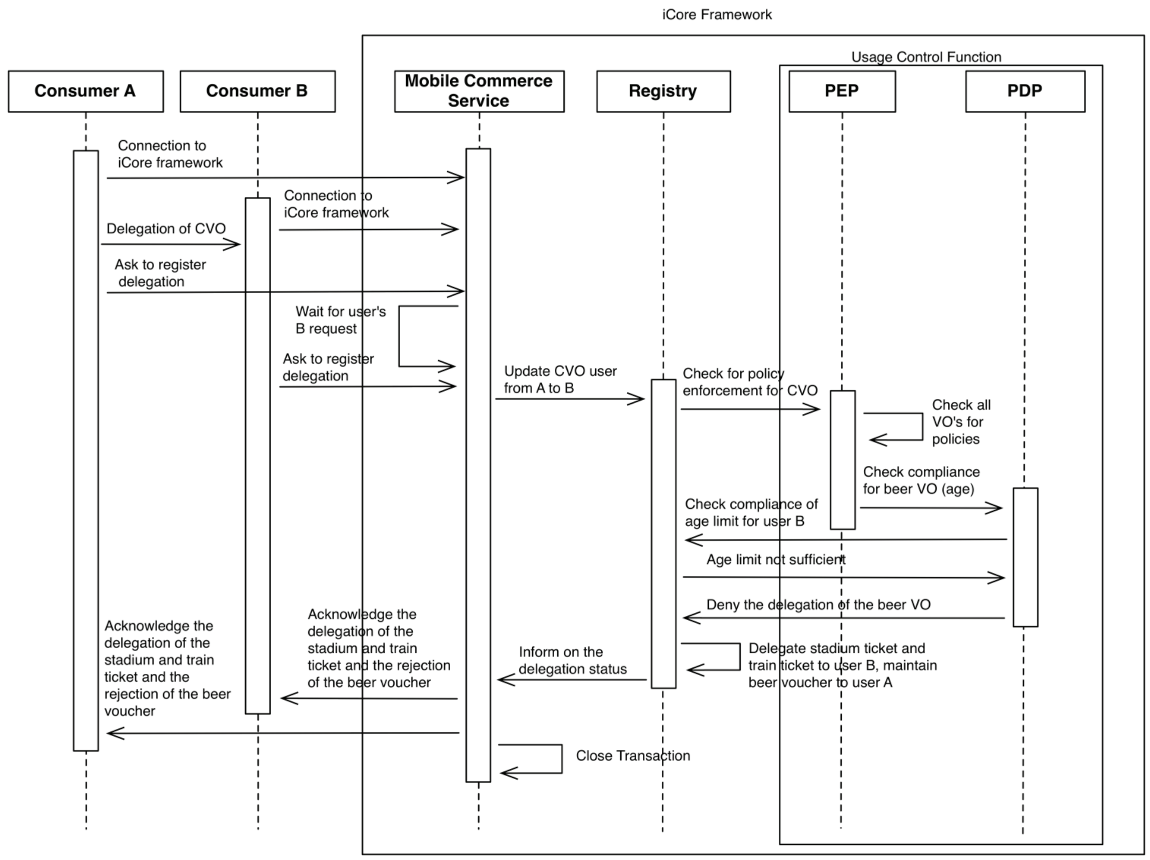
iCore Framework
Usage Control Function
Consumer A
Consumer B
Mobile Commerce Service
Registry
PEP
PDP
Connection to iCore framework
Connection to iCore framework
Delegation of CVO
Ask to register delegation
Wait for user's B request
Ask to register delegation
Update CVO user from A to B
Check for policy enforcement for CVO
Check all VO's for policies
Check compliance for beer VO (age)
Check compliance of age limit for user B
Age limit not sufficient
Deny the delegation of the beer VO
Delegate stadium ticket and train ticket to user B, maintain beer voucher to user A
Inform on the delegation status
Acknowledge the delegation of the stadium and train ticket and the rejection of the beer voucher
Acknowledge the delegation of the stadium and train ticket and the rejection of the beer voucher
Close Transaction

Figure 7: Workflow of a delegation of CVO, enforcing the age policy.

Citation: Löschner J, Baldini G, Kounelis I, Neisse R (2015) The Use of Policy Regulated Frameworks to Secure Mobile Commerce. Int J Multimed 1(1): doi: http://dx.doi.org/10.16966/ijm.101

the users and is supported by the enforcer user role. The latter can only be revealed in case a court order is issued and thus the iCore administrator must conform to such orders.

The workflow in such case is the following (Figure 8):

- The procedure until the independent check on each VO is exactly the same as described in the previous subsection.
- When the PEP detects a potential misbehavior, as already defined by the law enforcements in the policy database, it informs the m-commerce service. In this use case, the event is triggered as the delegation of the stadium ticket VO is been exchanged only a few minutes before the beginning of the match. As a result the authorities may have to deal with a case of black market purchase.
- The m-commerce service, which acts as the interface to the iCore framework, immediately notifies the law enforcer. In this notification, all the relevant information is included. Such information is the pseudonyms of the users, the values of the tickets (event, seats, price, etc.), accompanied VOs, etc.
- As the act itself (the delegation) is not directly forbidden by any policy, the procedure inside the iCore proceeds as planned. In the meantime the law enforcers have all the necessary data in order to investigate the case. If the case is proven to be illegal and a court order is issued, the law enforcements can formally ask for the full details of the transaction.

Comparison with Other Frameworks for Secure M-Commerce.

The proposed framework is able to mitigate some of the security identified by Wang, et al. in [15]. In particular, the iCore framework can support the payment completion invariant described in [15], where the information of payment of an Item must be preserved among the participating parties in the m-commerce scenario: Merchant, Shopper and Cashier. With reference to the challenges described in [15], the proposed framework is able to mitigate:

- Diversity in the adversary's roles, where merchant, shopper and cashier can mimic each other's role. Roles are clearly specified in the iCore framework for all the authenticated and authorized parties and the access to the data (i.e., VO) for reading, modification and deletion are clearly defined in the sticky policies associated to the VO.
- Confusion in coordination, where the merchant, shopper and cashier can have a partial view of the overall transaction. As described in Mobile Commerce section, the iCore framework regulates the creation and access to the VOs and the overall transaction is controlled by the iCore framework.

In addition, the iCore framework is able to protect the privacy of the users because the users profile is stored in VO as well, with their own sticky policies.

In [16], the authors describe a framework for m-commerce with special focus on security requirements. The framework is based on a credit model to resolve the security issue of mobile agent based electronic transactions. Protection against malicious agents is implemented using a credit assessment model, which basically evaluates the reputation of an agent, which wants to execute an m-commerce transaction. In this article, the credit assessment model is basically implemented with the authentication and usage control mechanism described in Policy Enforcement section while [16] does not address the protection of the data of the m-commerce transactions or delegation of rights from an user to another, which is instead described in this article.

The authors in [17] describe the application of access control models to the m-commerce context in similar way to this article. Both papers also share the same objective to provide design solutions for m-commerce where distributed organizations and individuals want to work together and share their information but they also need to protect their privacy

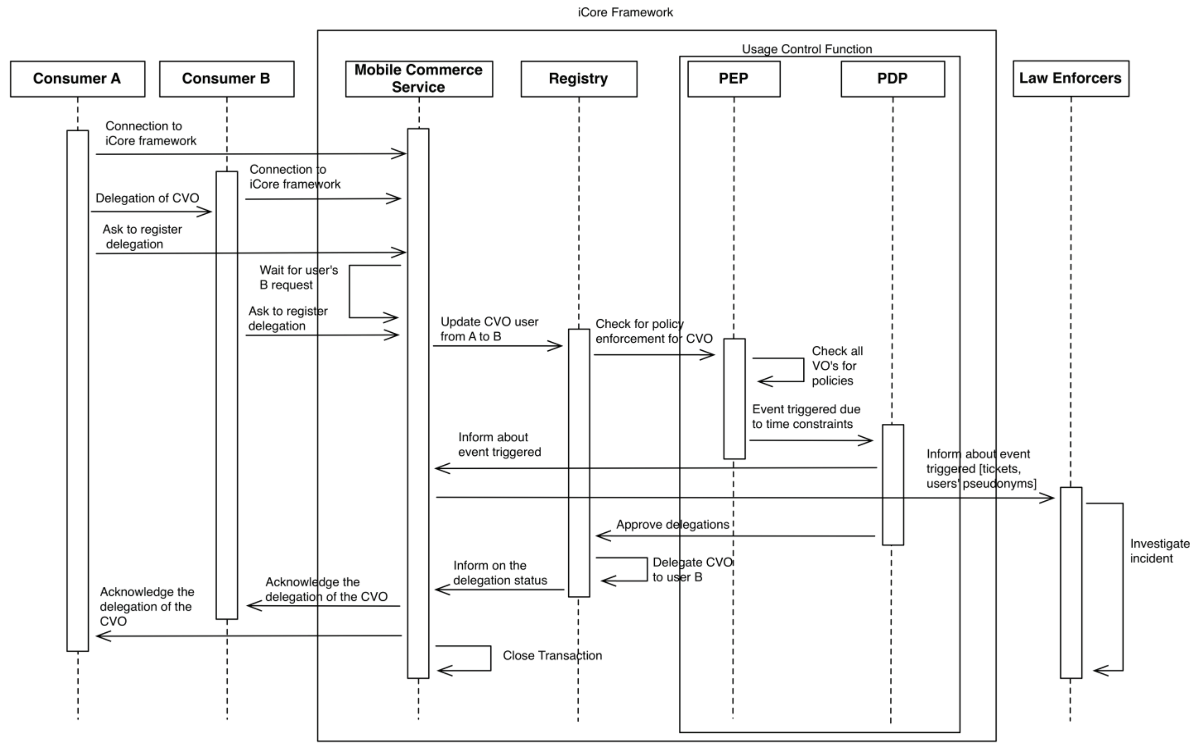
iCore Framework
Usage Control Function
Consumer A
Consumer B
Mobile Commerce Service
Registry
PEP
PDP
Law Enforcers
Connection to iCore framework
Connection to iCore framework
Delegation of CVO
Ask to register delegation
Wait for user's B request
Ask to register delegation
Update CVO user from A to B
Check for policy enforcement for CVO
Check all VO's for policies
Event triggered due to time constraints
Inform about event triggered
Inform about event triggered [tickets, users' pseudonyms]
Approve delegations
Investigate incident
Delegate CVO to user B
Inform on the delegation status
Acknowledge the delegation of the CVO
Acknowledge the delegation of the CVO
Close Transaction

Figure 8: iCore framework and interaction with law enforcers in case of suspicious incident.

and sensitive information and establish proper protocols for access and sharing activities. The authors in [17] propose a combination of role-based, group-based, task-based access control (RGT-based access control) to address the different needs of the user. The RGT-based access control is complemented by authentication and authorization functions and it is integrated in an overall layered framework for m-commerce similar to the one presented in 5 A Voucher Use Case and Workflow section of this article, even if the concept of VO/CVO is not presented. While the models proposed in the two papers are very similar (based on access control), this paper introduces the following concepts in comparison to [17]:

- The encapsulation of data in VO is not presented in [17], even if the concept of a virtual environment where access control could be enacted is presented.
- Policy Enforcement mechanism can be used to enforce policies in additional to access control rules.
- This paper presents also the case of delegation of access control.

The application of RBAC to the e-commerce context is presented in [18], where an object-oriented approach is also introduced, which is very similar to the iCore framework, because VO/CVO is basically stored as objects. This article introduces a more sophisticated usage control framework than the RBAC model used in [18].

A framework based on RBAC with policies is also presented in [19], where an extension of RBAC is used to define User Group Role (UGR) for e-commerce applications. The framework is implemented using XACML Policy language in combination with RBAC. The proposed architecture is very similar to the framework presented in this article as PEP and PDP components are also used. The model proposed in [19] does not support delegation as discussed in this article and it does not use an object oriented model, but this could be easily extended. In contrast to the XACML policy language that only supports attribute and propositional operators, the language we adopt in our framework has more expressiveness and supports temporal, cardinality, and event operators. Simple policies that can be expressed using our language like “block and account after 3 failed logins” cannot be expressed using XACML.

Conclusions and Future Developments

In this article we addressed important issues in m-commerce related to the lack of security and privacy of the customer through a policy based framework. In addition, we addressed the heterogeneity of m-commerce technologies and the fragmentation of m-commerce transactions through the concept of Virtual Object (VO), which can encapsulate all the m-commerce transaction data. These concepts have not been proposed or used in limited way in previous m-commerce studies. We have evaluated the proposed concepts and framework in practical scenarios, which involve different domains to verify their feasibility.

Future work will focus on the verification and validation of the proposed architecture using modelling and simulation methods and prototypes implemented with standards languages and tools (e.g., XACML). In addition, we will investigate the possibility to apply the policy based framework to the customization and profiling of the customer to enhance m-commerce efficiency and security. An example of the application of this concept in IoT environment is provided in [20].

Acknowledgment

This work was funded by the EC through the FP7 project iCore (287708) [11].

References

1. Varshney U, Vetter RJ, Kalakota R (2000) Mobile commerce: a new frontier. Computer 33: 32-38.
2. Dahlberg T, Mallat N, Ondrus J, Zmijewska A (2008) Past, present and future of mobile payments research: A literature review. Electronic Commerce Research and Applications 7: 165-181.
3. Lin HF (2013) Determining the relative importance of mobile banking quality factors. Computer Standards & Interfaces 35: 195-204.
4. Vlacheas P, Giaffreda R, Stavroulaki V, Kelaidonis D, Foteinos V, et al. (2013) Enabling smart cities through a cognitive management framework for the internet of things. IEEE Communications Magazine 51: 102-111.
5. Pearson S, Casassa-Mont M (2011) Sticky Policies: An Approach for Managing Privacy across Multiple Parties. Computer 44: 60-68.
6. Nilashi M, Ibrahim O, Mirabi VR, Ebrahimi L, Zare M (2015) The role of Security, Design and Content factors on customer trust in mobile commerce. Journal of Retailing and Consumer Services 26: 57-69.
7. Belanger F, Hiller JS, Smith WJ (2002) Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. J Strateg Inf Syst 11: 245-270.
8. Rayport J, Jaworski B (2001) Introduction to E-Commerce. McGraw-Hill, New York.
9. Liu J, Kauffman RJ, Ma D (2015) Competition, cooperation, and regulation: Understanding the evolution of the mobile payments technology ecosystem. Electronic Commerce Research and Applications.
10. Kounelis I, Baldini G, Muftic S, Loschner J (2013) An Architecture for Secure m-Commerce Applications. 19th International Conference on Control Systems and Computer Science (CSCS) 519-525.
11. iCore (2011) FP7 Integrated Project. iCore FP7.
12. Srinivasan N, Paolucci M, Sycara K (2006) Semantic Web Service Discovery in the OWL-S IDE. Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS) 6: 109b.
13. Neisse R, Pretschner A, Di Giacomo V (2011) A Trustworthy Usage Control Enforcement Framework. Sixth International Conference on Availability, Reliability and Security (ARES) 230-235.
14. ABC4Trust (2012) Attribute-based Credentials for Trust.
15. Wang R, Chen S, Wang X, Qadeer S (2011) How to Shop for Free Online--Security Analysis of Cashier-as-a-Service Based Web Stores. Proceedings of the 2011 IEEE Symposium on Security and Privacy 465-480.
16. Wei D, Wei J (2010) Research on the Security of an Improved E-commerce Model. International Conference on E-Business and E-Government (ICEE) 2534-2537.
17. Kim S, Zhu J, Smari WW, McQuay WK (2006) Security and Access Control for a Human-centric Collaborative Commerce System. International Symposium on Collaborative Technologies and Systems 429-439.
18. Hongxin L, Keqing G, Yugang W (2010) The Application of RBAC Model in E-Commerce System. International Conference on Electrical and Control Engineering (ICECE) 3059-3062.
19. Shao L, Qin A, Zheng X, Zhang J (2012) Improvement and Implementation of RBAC Access Control Model. International Conference on Management of e-Commerce and e-Government (ICMeCG) 110-115.
20. Kounelis I, Baldini G, Neisse R, Steri G, Tallacchini M, Guimaraes Pereira A (2014) Building Trust in the Human-Internet of Things Relationship. IEEE Technology and Society Magazine 33: 73-80.