ARES CONSOLIDER INGENIO 2010 CSD2007-00004

WP3.T2 Design of anonymous payment systems implementable on national or corporate electronic ID cards.

Arnau Vives-Guasch and Jordi Castellà-Roca

Universitat Rovira i Virgili
Departament d'Enginyeria Informàtica i Matemàtiques
Avda. Països Catalans, 26
43007 Tarragona (Catalonia, Spain)
{arnau.vives,jordi.castella}@urv.cat

Abstract. The electronic ticketing (ET) and automatic fare collection systems (AFC) can reduce economic costs and time intervals in a wide variety of transport systems. For exemaple. the paper costs reduction and the improved processes are arguments to adopt the ET. The AFC systems can be used to improve the control of the infrastructures using a management strategy of infrastructures depending on the passenger ows. Nonetheless, there exist privacy threats to which users are ex- posed when they use ET and AFC systems. Anonymity of users is not always guaranteed and users can be traced. We have classied and described the main proposals in each field (ET and AFC). Finally, we conclude with our published works in the two lines of research.

1 Introduction

Information technologies (IT) are constantly evolving our day-by-day operations in our society. Transport is one of the sectors where IT take an important role. Nowadays, it is possible to receive information easily about different journeys, even booking them at home.

Most Intelligent Transport Systems (ITS) can benefit from the latest technological improvements. ITS add information and communication technologies to transport infrastructures and vehicles, thus providing advantages as costs reduction, time optimization, safety improvement and even inter-vehicle alarm communication. Electronic Ticketing (ET) and Automatic Fare Collection (AFC) systems suit in these ITS by using documents in electronic format that can speed up all their processes, reduce costs, and even enable the monitorization of the traffic's density in real-time.

Electronic ticketing (ET) systems become more oriented to scheduled transport, as the user publishes in advanced his/her destination. These systems are used for many different sectors and services, such as the air travel industry, public transport, or even leisure and determined events. Considering the case of transport e-ticketing systems, user's check-in and check-out could be controlled in order to verify the ticket and also if the service has been used accordingly to this ticket information.

In addition to these initiatives, the International Air Transport Association (IATA) started in 2004 a programme to introduce the use of electronic tickets [25] which finished in 2008. The no necessary use of paper tickets reduced the costs by $3000M US dollar [26], boosting disintermediation by using electronic tickets. Another example of that is the electronic air flight boarding pass. Vodafone and Spanair [50] made a test in 2007 where passengers received their electronic boarding passes into their mobile phones. Other companies like Air Canada [1] or Continental [41] followed the same direction and they offer similar services to their customers.

Electronic tickets has been used in other transport services. In this way, the AMSBUS [3] booking system from the Czech Republic allows the purchase of SMS tickets. First, the passenger receives the ticket into the mobile phone. Then, he/she shows the message to the ticket inspector when she is instructed to do so. In Denmark, the same kind of service is provided by Fynbus [18].

Ticketing systems can be applied to different services as leisure events (museum, cinema, theatre, sport event) and also for transport services (bus, train, air plane, subway). For instance, Leeds United [31] supporters can book a match and later receive an SMS with the booking confirmation together with some added information such as their assigned seats.

Automatic Fare Collection (AFC) systems become more oriented to mass and *short-distance* public transport, as the user does not make public in advanced his/her destination, and the fare is calculated depending on the place where the user checks in and out of the system. For this reason, a (rechargeable) prepaid wallet with a minimum balance is needed.

One of the main issues of both AFC and ET transport systems is the privacy of their users. Anonymity of users is not always guaranteed (for honest users), and there appears the problem of ticket tracking, and the real possibility in some systems to link the ticket to a certain user. Then, not only privacy would be violated; user identity could be revealed and all his/her entering and exiting movements in these systems could be also tracked. Users logically prefer total anonymity in order not to show any of their movements; system administrators and police/security forces prefer no existance of privacy for users. The option of a privacy-preserving transport system that could satisfy the two parties would be revocable anonymity for users, enabling then this revocation for dishonest users or emergency situations. Tracking of the ticket would have to be limited to the entrance and its corresponding exit (1 use), with no possibility to link it neither with other uses by the same device nor the identity of its user.

1.1 Document organization

In section 2 we define, classify and describe the main proposals of electronic ticketing (ET). Next, in section 3, we perform a security analysis of the AFC proposals that consider revocable anonymity and, classify them accordingly the untraceability property. Finally, we outline the conclusions and enumerate our contributions in section 4.

2 Electronic tickets

We perform in the following section an analysis of the e-ticketing systems, first defining the involved participants, phases, and the most suitable services for these systems; the security requirements of the e-ticketing systems are evaluated in section 2.1 the classification of the proposals is detailed in section 2.2 and, finally the e-ticket information is described in section 2.3.

We introduce the participants who are involved in an electronic ticketing system, according to authors [15, 36, 39, 37, 45]:

- User: receives the electronic ticket and sends it for its validation in order to use the service.
- Issuer: issues the electronic ticket to the user. It could be also the same service provider or the intermediary [48].
- Service provider: receives the e-ticket from the user and validates it. If correct, then it gives the service to the user.

These are the general participants, as some systems include other participants. For example, the shop or the broker [15, 29, 56]. Also in some public key cryptography (PKI) systems [42, 46], the Certification Authority (CA) is also included. In [47], the e-ticketing system is based on the use of Smart-Cards, and the Smart-Card issuer is also included to the system. The scheme presented in [12] includes a user agent and the network access service provider. The system proposed in [27] includes user localization, as well as information related to this location. In order to give this service preserving user anonymity, the network provider is added as a true participant. The system also considers the possibility to get the e-ticket, and the payment service provider, the bank and the credit card issuer are also considered as participants involved in the system.

According to authors, an electronic ticket system consists of three main phases: e-ticket payment, issue and validation [13, 15, 47, 48, 29, 37, 5, 45, 12]. However, these three phases are not unanimously defined. Some authors [42, 43, 36, 39] group payment and issue phases, converting from three to two e-ticket phases: e-ticket payment and validation. Other proposals [58, 4, 9] add a previous registration phase in which users must be identified and authenticated in order to give them permission to use the service. In [23], as well as the previous phases, service start and end are considered as true phases too. This real disagreement in electronic ticket phases is due to the great number of types of services where e-tickets could be used [16, 5].

The existing proposals have been evaluated depending on the services that could be offered with these systems. Since the study (see Table 1), one of the most relevant facts is that electronic ticketing systems are mainly oriented to public transport services. Most of these transport services are rail transport [42, 13, 20, 51, 22, 23, 27, 7, 32, 21], followed by air travel [5, 56, 19, 50, 1, 7, 55, 46, 41], bus transport [42, 13, 23, 44, 18, 7, 32, 3] and subway [42, 13, 51, 23, 7, 32], with one

solely proposal used for taxi transport [7]. In 2006 in Germany, more than 25 e-ticketing projects were intended or in testing phases for public transport [21], which most of them were thought for short distance journeys. Running systems applied to tolls [38, 37, 51, 7, 32] are closer to electronic payment systems than electronic ticketing systems. Users pay for the service when they use it, charging the amount of money directly to the current or credit card accounts. The rest of the proposals are oriented to the leisure sector [42, 30, 29, 5, 31, 7], as sports or cultural events.

SERVICES	Air travel	Rail	Bus	Subway	Taxi	Tolls	Leisure
[38]						✓	
[42]		✓	✓	✓			✓
[13]		✓	✓	✓			
[30]							✓
[29]							✓
[20]		✓					
[37]						✓	
[51]		✓		✓		✓	
[5]	✓						✓
[56]	✓						
[22]		✓					
[23]		✓	✓	✓			
[19]	✓						
[50]	✓						
[1]	✓						
[44]			✓				
[18]			✓				
[27]		✓					
[32]		✓	✓	✓		✓	
[7]	✓	✓	✓	✓	✓	✓	✓
[31]							✓
[55]	✓						
[41]	✓						
[3]			✓				
[21]		✓					
[46]	✓						
TOTAL	9	10	8	6	1	5	6

Table 1. Services for electronic ticketing systems

2.1 Security requirements

In general terms, e-tickets should achieve the following requirements [42, 36]:

- Reduced size: e-tickets are commonly stored in mobile devices like mobile phones or Smart-Cards. These devices have a reduced storage capacity and then electronic ticket size should be small.
- Flexible: e-ticket could be used in several services and systems without modification needs.

- Secure: e-ticket security is considered as one of the main aspects to be achieved.
- Ease of use: e-tickets should be used easily, no more difficult than the use of paper tickets.
- Availability: systems must put up with hard conditions, assuming that electronic tickets could be used every time. For example, a huge number of users could all be connected to the system during the primetime, and this system should be well-structured in order to avoid system collapse.
- Payment system: in [36] the system is required to include possible payments on the spot.
- Efficiency: every process of e-ticket phases, especially verification, must be quick. The system should avoid a possible process delay.
- Portability: e-ticket could be sold and used in different scenarios and under several conditions [48, 4, 9].

Moreover, the following security requirements have to be also achieved:

- Authenticity: e-tickets should take measures to avoid falsification. A user could verify the authenticity of the ticket.
- Non-repudiation: once the issuer sends the ticket to the user, there is no possibility to deny this emission.
- Integrity: once the ticket has been issued, it cannot be modified at all.
- Anonymity: anonymity could be provided or not depending on the service. There are three considered anonymity degrees:
  - Anonymous: user could use the service without identification. The system guarantees no link existence between user and ticket.
  - Non-anonymous: the service requires user identification and authentication. It would be useful for services with security control area (e.g. plane flights), or services which require user recognition.
  - Revocable anonymous: the service is anonymous, but ticket tracing is stored in the system. Afterwards, this anonymity could be broken, revealing user's identity. It would be useful for overspending control or other major causes.
- Transferability: tickets could be personal or transferable:
  - Transferable: some services allow ticket transferability.
  - Non-transferable: ticket transferability could be forbidden for some services (e.g. plane flight).
- Reusability: a ticket could be used once or many times depending on the terms and conditions of each ticket.
  - Non-overspending: e-ticket could be used only once.
  - Reusable: ticket could be used a preset number of times, or indefinitely until a preset date.
- Online/Offline: on online systems, ticket verification requires connection to the system. On the other hand, if ticket verification does not require system connection, the system is classified as offline. Before-use verification is also classified as an online system, and after-use verification is classified as an offline system [5].

– Expiration date: the system is able to detect the compliance of the expiration date of the ticket.
– State: the ticket includes its state information, or alternatively a link to get this information.

Issuer's ticket digital signature provides basic requirements: authenticity, non-repudiation and integrity [16, 13, 15, 40, 48, 5, 56, 22, 45, 28, 4, 9, 12].
Proposal in [28] provides true anonymity for the user by using Chaum's blind signatures [10]. Systems that provide revocable anonymity [42, 16, 40, 48, 5, 56, 58, 45, 23, 27] are mainly based on the use of pseudonyms.
smart-cards or mobile devices (mobile phones, smart phones or PDAs) provide ease of use in operations for e-ticketing systems. Personal Trusted Devices (PTDs) establish a secure communication channel with the validation system, doing the most sensitive operations securely and banning access to the user. Electronic ticketing systems which use PTDs are [42, 13, 30, 36, 47, 48, 58, 5, 22, 28, 9, 12, 27, 21, 2].
In [56], a signature intermediary [34, 35] is used to issue e-tickets. This intermediary could be the travel agency, and it could be allowed to issue signed e-tickets for air travel companies. This fact provides system decentralization as well as it guarantees security. Users could verify their received e-ticket validity with no need of communication to the end service provider.

Table 3 shows different proposals of e-ticketing systems and their achieved security requirements.

ATH	Authenticity	TF	Transferable
NRP	Non-repudiation	NTF	Non-transferable
IT	Integrity	NOV	Non-overspending
AN	Anonymous	REU	Reusable
NAN	Non-anonymous	ON	Online
RAN	Revocable anonymous	OFF	Offline
EXD	Expiration date	ST	State

Table 2. Relationship between the name of the security requirement and its code

2.2 Existing security proposals

The analyzed proposals could be classified depending on several security requirements as: anonymity, transferability, reusability or verification type (online/offline).

In the following sections, the studied proposals have been classified depending on the anonymity compliance. Firstly, in section 2.2, anonymity-compliant schemes are described. The schemes that comply with anonymity, but enable

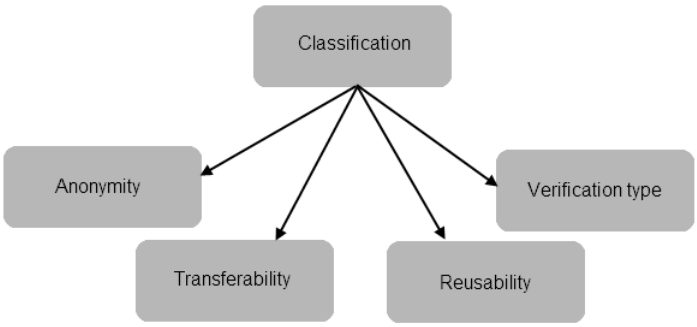

Fig. 1. Possible classifications of the proposals

user identification disclosure if needed (by overspending or law cases), are described in section 2.2. Finally, the schemes that do not comply with anonymity at all are detailed in section 2.2.

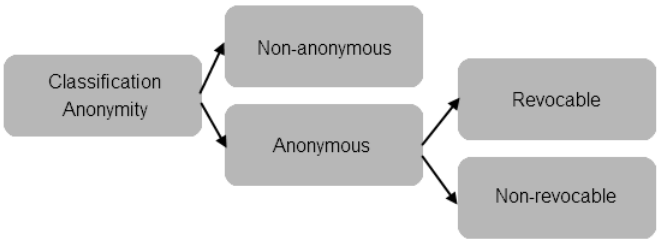

Fig. 2. Classification of the proposals by anonymity

Anonymous schemes In [14], Fan and Lei made an e-ticketing system proposal for electronic voting purposes. They use Chaum's blind signatures in order to achieve anonymity. Only two types of participants take part in the system: the authority and a group of voters.

PROPERTIES	ATH	NRP	IT	AN	NAN	RAN	TF	NTF	NOV	REU	ON	OFF	EXD	ST
[42]	✓		✓			✓		✓	✓		✓			
[16]	✓	✓	✓			✓	✓			✓	✓			✓
[13]	✓				✓		✓		✓		✓			
[40]	✓	✓	✓		✓	✓		✓	✓			✓		
[43]	✓		✓		✓			✓	✓	✓	✓			
[36]	✓	✓	✓		✓		✓		✓	✓		✓		
[47]	✓		✓		✓		✓		✓	✓	✓			
[48]	✓	✓	✓		✓	✓	✓		✓		✓	✓		
[39]	✓				✓			✓	✓		✓			
[29]	✓		✓		✓		✓		✓	✓	✓			
[5]	✓	✓	✓		✓	✓	✓		✓	✓	✓			
[56]	✓	✓	✓			✓		✓	✓		✓			
[58]	✓					✓		✓	✓		✓			
[22]	✓	✓	✓	✓				✓	✓		✓	✓		
[28]	✓	✓	✓	✓				✓	✓		✓			
[45]	✓	✓	✓		✓	✓	✓		✓			✓		
[4]	✓	✓	✓		✓			✓	✓		✓		✓	
[9]	✓	✓			✓		✓				✓		✓	✓
[23]	✓					✓	✓			✓	✓	✓		
[12]	✓	✓	✓	✓				✓	✓			✓		
[27]					✓	✓	✓		✓		✓	✓	✓	

Table 3. Comparison of e-tickets' security requirements (see the codes at Table 2)

Song and Korba [49] propose a system for payment of services, providing strong privacy (anonymity) and non-repudiation. This system achieves overspending control, protection against ticket loss or stealing, without transferability option. Anonymity is achieved by using Chaum's blind signatures.

Haneberg et al. [22] present an electronic onboard ticketing scheme, by using a PDA connected to the system through Bluetooth and using Java for all applications. PDAs are chosen for their short-range wireless communications and the display. Anonymity is achieved in this proposal as no personal data is needed, and anonymity then only depends on the payment method used.

In [45], Quercia and Hailes' e-ticketing system proposal is based on Chaum's e-cash blind signatures, providing anonymity to the user, but the communication cost could be high, and possibly slow down the system. Apart from anonymity, non-repudiation, offline verification as well as portability are achieved in this proposed system.

The great majority of the described proposals that comply with anonymity are based on Chaum's blind signatures [11].

Revocable anonymous schemes In the proposal of Patel and Crowcroft [42] the security requirements are defined, where revocable anonymity is achieved, as well as offline mode, although central authority intervention is needed in order to prevent overspending.

Depending on the services, anonymity, transferability or reusability would be re-

quired in the Fujimura et al. proposal [16]. Pseudonyms are proposed if anonymity is required, and overspending is controlled by a central database (online mode).

Wang et al. in [58] presented a system that is revocable anonymous, where the authentication method is made by the use of a smart-card.

In [23], Heydt-Benjamin et al. made a proposal using latest advances in e-cash to improve privacy in electronic ticketing systems for public transit. It uses pseudonyms in order to achieve anonymity.

Chen et al. [12] propose the use of mobile devices (mobile phones, smart phones or PDAs) in e-ticketing systems, by taking advantage of their wireless communications. They focus on the compliance of several security requirements, as (revocable) anonymity, non-repudiation, as well as efficient verification. The ticket process is defined in 3 phases in the paper: request, issue and verification. Anonymity is achieved by the use of pseudonyms.

The system defined in [27] by Jorns et al. is oriented to transport services, as the ticket includes route information. The system uses GPS technologies to show user's location. It is used with mobile phones and PDAs. Digital signatures are not used in this paper. Pseudonyms are used in order to achieve revocable anonymity.

Lutgen [32] defines security management system requirements of the German core application in public transport, as it requires integrity, traceability of all the participants involved in the system, and the possibility to block the user in order to limit damage. Then, as this system could achieve traceability, anonymity could not be guaranteed.

Serban et al. [46] present an e-ticketing system. This system is oriented to air travel e-tickets. A certification authority (CA) is needed to authenticate all participants in the system (sellers, airlines, banks, reputation server) except for users. Users in the system do not have to be authenticated then, but credit card payment information is only sent to the bank, as anonymity could not be guaranteed to the user if overspending has been attempted.

The Vives-Guasch et al. [54] and Castellà-Roca et al. [8] works present two e-ticketing systems that include the exculpability requirement, i.e. the service provider cannot falsely accuse the user to have overspent the ticket, and the user is able to demonstrate that she has already validated the ticket before using it. These proposals comply with revocable anonymity, as the user identity could be revealed if the user tries to overspend the ticket or for other security reasons. In addition accordingly to the authors, the e-ticketing systems are in process to be developed as a first prototype through using mobile devices for the users with Near-Field Communication contactless technology.

The majority of the studied proposals use pseudonyms in order to achieve revocable anonymity. If pseudonyms are used, real identity information is not put into the ticket, only its pseudonym. But if the issuer could link every pseudonym to its real identity, then anonymity could be compromised. For that reason, only revocable anonymity for the user could be achieved. In this scenario, user traceability could be easily performed if user does not change its pseudonym regularly because the same pseudonym would be used for different tickets. Certain volume of data could allow all the involved participants to make user profiles if there were no pseudonym controls.

Non-anonymous schemes In Elliot's article [13], anonymity is not considered for travel services, and it focuses mainly on the use of smart-cards to store and manage the electronic tickets.

Pedone [43] applied atomic broadcast to e-ticket validation system, where distributed databases could reply to user requests more rapidly, improving server availability as well as avoiding bottleneck problems, as information is replicated in the distributed servers. Two phases are defined in this paper: e-ticket reception and verification.

According to Kuramitsu et al. [30], this paper presents an electronic ticketing system that allows transferability between two tamper-proof devices (smart-cards, or alternatively mobile devices that have an internal smart-card). This transfer process guarantees atomicity, which means that the ticket will be totally transferred or not transferred. No digital signature is used to sign the ticket, there is protection only when the e-ticket is transferred by using a secure channel between the two devices.

In [47], the e-ticketing system uses a smart-card (SIM card of the mobile phone), which defines four participants (merchant, customer, card issuer and service provider) and three process phases (ticket issue, transfer and verification). The ticket is digitally signed, and its verification is done online. Transferability is also allowed through a TTP.

In [36], Maña et al. perform a project where e-tickets are stored in the SIM card of the mobile phone. Their scope is oriented to have offline verification, non-anonymity, transferability and portability. The ticket is linked to a user identification, and then, anonymity cannot be achieved.

Kuramitsu and Sakamura [29] presented a system that uses contactless smart-cards to store e-tickets. The system accesses the database (access control), and checks ticket validity. If the ticket is valid, the user is authorized to access the event updating the database. This paper introduces severe limitations in smart-cards store capacity, as well as describing problems in contactless communication

disconnections (causing inconsistency), and also describing the need for use of standarized formats in order to solve the management of specific tickets from different applications. Three phases are defined in this paper: issue, selling and verification. This proposal provides transferability, but not anonymity.

In [37], Matsuo and Ogata present an e-ticketing system that could fit with Electronic Toll Collection (ETC). It consists of a prepaid system, where the ticket is already received. Then, the user only has to send the ticket for its validation. Smart-cards are used in this scenario for their tamper-proof properties. Wireless communication technologies are used for the transaction. Space and time synchronization is also taken into account for the ETC system, as it uses GPS. This paper considers the existence of three phases: issue, spend, recharge; as well it considers three participants in the system: issuer, user, and the shop. Instead of the use of digital signatures for e-ticket verification, the system uses hash functions to minimize verification delays although several security properties could not be achieved.

In [5], either the user or the e-ticket should be identified in order to prevent problems such as malicious attacks. There is a real relationship between anonymity and transferability for user and e-ticket identification and reusability is also considered for other ticket information, such as its destination. Online mode is used in this scheme for security reasons, as they say offline systems show weaknesses to malicious attacks.

The proposal by Wang et al. [56] present an air ticket booking scheme where air travel companies delegate their issue digital signatures to a proxy. This proxy is responsible for signing the ticket. Users could verify integrity and authenticity, as well as the verification of the e-ticket's issue delegation from the air travel companies to the proxy. In this paper, only basic requirements are considered, anonymity and other security requirements are not taken into account.

In [9], Chang, Wu and Lin present an e-ticketing system for mobile users, considering security aspects like ticket theft or verification of the ticket owner, all in online mode. It uses hashes that are unknown to the issuer authority in order to achieve these security requirements. These tickets are digitally signed and can also be transferred to another user always with the participation of the TTP. Anonymity is not achieved as every ticket has its identifier, and overspending is controlled by searching on the central database. It has also information of the ticket's expiration date.

In [21] Haneberg presents applications for railway tickets (transport), taking into account advantages and disadvantages in the properties that smart-cards, PDAs and mobile phones have, focusing on their tamper-proof security requirements. Overspending is controlled by a central server (online mode), and anonymity is not considered in this system.

In these systems, anonymity could not be achieved due to different reasons. Some proposals are oriented to services where anonymity could not be provided to the user, or simply, these systems are not conceived to achieve anonymity at all. Some systems do think about e-ticket transferability, and in the majority of the cases, anonymity could not be achieved because the ticket is already digitally signed, without possibility to modify e-ticket information.

2.3 Information

Like classic paper tickets, electronic tickets would have to include some basic information for its practical use. In this section, information fields that electronic tickets would have to include are briefly described:

- Serial number: unique identification of every ticket.
- Issuer: entity who is responsible for issuing the ticket. This issuer could be also the service provider, or the intermediary.
- Service provider: entity who offers the service to the user.
- User: information about the e-ticket owner. In case of existence of this field in the e-ticket, user anonymity could not be achieved.
- Service: description of the service contract.
- Terms and conditions: definition of the e-ticket terms and conditions, or alternatively an external link to enable consultation.
- Type of ticket: ticket includes a field describing its type.
  - Transferability: if this field is permitted, transferability to another user is allowed.
  - Number of uses: information about the allowed number of ticket uses.
- Destination: this field is used for transport services in order to have user destination information.
- Attributes: other attributes of the ticket that depend on the service (e.g. theatre seat).
- Validity time: it includes two timestamps, the starting and the expiration dates.
- Date of issue: e-ticket date of issue. Validity time field could be set by means of including this field together with the terms and conditions.
- Issuer's digital signature: e-ticket issuer has a PK cryptosystem key pair, being able to digitally sign the e-ticket.
- Device identification: e-ticket is linked to a specific device.

Table 5 shows the information field that some e-ticket proposals include. Fields are differently defined depending on the e-ticket service.

3 Automatic Fare Collection

The actors involved in any Automatic Fare Collection (AFC) system are the users, the service providers and the payment authorities. Users ($\mathcal{U}$) access to the transport system and pay for the received service at the exit. The service providers ($\mathcal{P}_\mathcal{S}$ source station, $\mathcal{P}_\mathcal{D}$ destination station) control the tickets used by $\mathcal{U}$s. $\mathcal{P}_\mathcal{D}$ also verifies if the $\mathcal{U}$ direction is coherent with the ticket. The users travel in one direction so that a entrance ticket must be obtained in a station placed before the destination station according to the direction. Thus, the $\mathcal{P}_\mathcal{D}$ rejects an entrance ticket if it has been obtained in a station that is after the destination station. Finally, payment authorities ($\mathcal{M}_\mathcal{C}$) manage all the user's payments when they exit from the system.

AFC systems usually have two phases: system entrance and system exit. In the system entrance, users join in the source station and receive an entrance ticket from $\mathcal{P}_\mathcal{S}$ that will have to be showed in the destination station. The users show the entrance ticket when they exit of the system (system exit). $\mathcal{P}_\mathcal{D}$ then calculates the fare that $\mathcal{U}$ must pay. If all the process is correct, the user receives an exit ticket, which is an evidence that proves that the user has followed the protocol correctly. Nonetheless, there is an optional phase of registration, i.e. there are AFC systems that do not consider the user registration. In this phase, the users provide their credentials, in order to prove their identity effectively.

Next, in section 3.1 we perform an security analysis of AFC proposals that consider revocable anonymity for users, the proposals are classified in section 3.2 and the information of the AFC tickets is finally described in section 3.3.

3.1 Security requirements

Transport services give a receipt or a ticket to users in order to be further verified; this receipt is a proof that the protocol was followed correctly. In these electronic systems, the following security requirements have to be guaranteed:

- Authenticity: a ticket must be generated by its authorized issuer.
- Non-repudiation: the issuer can not deny the emission of one of its tickets.
- Integrity: the ticket, once generated, can not be further modified.

SN	Serial Number	IS	Issuer
SP	Service Provider	US	User
SV	Service	TC	Terms and Conditions
TT	Type of Ticket	TF	Transferability
NU	Number of Uses	DS	Destination
AT	Attributes	VT	Validity Time
DI	Date of Issue	DS	Issuer's Digital Signature
DV	Device identification		

Table 4. Table 5 caption

INFORMATION	SN	IS	SP	US	SV	TC	TT	TF	NU	DS	AT	VT	DI	DS	DV
[42]	✓	✓			✓	✓			✓			✓			
[16]		✓		✓		✓		✓	✓			✓		✓	
[17]	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	
[36]	✓			✓	✓	✓								✓	
[47]	✓	✓	✓		✓	✓			✓			✓	✓		
[48]		✓	✓	✓	✓	✓	✓								
[39]	✓	✓		✓	✓						✓	✓	✓	✓	
[5]	✓	✓		✓			✓			✓	✓	✓			
[58]	✓				✓								✓	✓	
[4]	✓	✓		✓								✓	✓	✓	✓
[9]	✓	✓	✓	✓								✓	✓	✓	
[27]	✓	✓		✓		✓	✓			✓		✓			

Table 5. Information on e-tickets (see caption in Table 4)

In addition to these basic requirements, the following ones must be also guaranteed:

- Validity time: Any ticket has a validity time parameter to check whether it is in force or not. Each spent ticket is stored in a database until its validity time has expired.
- Non-overspending: a ticket can only be used once. Before allowing the use of any ticket, its validity period is checked. If the verification is correct, the system checks that the ticket is not in the database of spent tickets by using its serial number. The verification ensures that the ticket is not used more than once.
- Revocable anonymity: the system must guarantee the user's anonymity in order to receive acceptance of the user community, but the system and the public authorities prefer non-anonymity for security and control reasons. Thus, an intermediate solution is revocable anonymity for users. If a user misbehaves, her anonymity is revoked.
- Non-traceability: the provider can only trace an entrance of a user with its corresponding exit, but can never trace different journeys of a same user, what could enable profiles generation.

3.2 AFC proposals

The previous AFC proposals with revocable anonymity can be classified depending on the untraceability or the device used. We have classified them in the following sections according to their traceability or untraceability, and, finally, we present a brief considerations about them.

Traceable Wang et al. [57] proposal can be used for different services. Depending on this service, some of the ticket information fields, such as user, service

Ref.	Anonymity	Untraceability	Device
[57]	Revocable	No	Mobile
[6]	Revocable	No	Smart-card
[23]	Revocable	Yes	Mobile and Smart-card
[24]	Revocable	No	Smart-card
[27]	Revocable	No	Mobile
[33]	Revocable	No	Mobile
[53, 52]	Revocable	Yes	Mobile

Table 6. Comparison of the analyzed proposals

provider and service identities could be filled or not, differentiating then two digital signature schemes: single signature scheme (when only one entity was involved in the ticket information) or multisignature scheme (when 2 or more entities were involved in the ticket information). There are four roles in the scenario: the *signer roles* are the involved entities in the system that will sign (or multisign) the ticket; the *trusted role* knows the secret values of the signer roles; the *verifier role* verifies the received ticket; and the *credential role* controls all the data associated with tickets and their users identified by pseudonyms. A credential centre takes the credential role, and it is the responsible of issuing a fixed pseudonym for each user as well as revoking the users' anonymity if necessary. As this credential centre is able to link a pseudonym with its user, it enables then the possibility to trace all the movements made by a certain user identifiable by a fixed pseudonym. Furthermore, this information is made public to anyone. Another problem is that the user cannot demonstrate that he has correcly done the verification (receipt).

In [6] Buttyán et al. present an AFC system that provides location privacy to users. The solution is based on the key-tree based approach together with the use of one-time identifiers (OTIs). The key-tree based approach belongs to symmetric key cryptography, and according to the authors, it makes it affordable for smart cards for their lower computation power requirements. It is used in order to reduce the high amount of keys that are generated in a symmetric key cryptographic system. OTIs are generated by the readers and sent to the cardholders, and are used in order to avoid linkage between some movements of the same card. The reader has a set of master keys, and when it receives the *card id* (pseudonym) from the cardholder, then, the new OTI is generated depending on the *card id* and the previous OTI_{i-1}. The new OTI_i is finally sent to the card. As the *card id* is known for the reader, tracking of the card could be easily achievable. Another problem is the need of synchronisation between the reader and the card through the OTI, as the need of knowledge of OTI_{i-1} in order to receive the new OTI_i from the reader allows that DoS attacks could be successful to break this correct synchronism. Finally, the user cannot demonstrate to a third party that she has correctly entered and exited the system.

In [24] Hong and Kang do a contribution of an AFC system for public transit using contactless smart cards, with its main issue in the protection of users' privacy. Users are already registered in a Trusted Third Party (TTP), which has all the information associated to them. Firstly, (1) a secure connection X.25 between the user and the TTP is established; (2) the user self-identifies and authenticates in this TTP, which (3) verifies then the correctness of the authentication, (4) gathers the user's privacy policy and the associated information from its distributed main repository (using the Shamir threshold sharing secret scheme) and (5) sends the necessary information to the user for possible future transactions. Card tracking is possible as one-time identification is not considered, and the TTP can recognize each movement made by a user. Users cannot also demonstrate the correct verification to a third party because he has no proof of the transaction.

The system proposed by Jorns and Quirchmayr [27] of an AFC system is oriented to transport ticketing systems, as the destination field is contained in the ticket information, and micropayments can be executed when travelling. The system is implemented for its use in mobile devices like mobile phones or PDAs, with J2ME technology. This system uses a set of pseudonyms for each user in order to avoid user tracking, and each pseudonym is one out of a chain of keyed hash values (HMAC), where each hash value is the result of the previous ones encrypted with this secret key. In the proposal, there is a *network provider*, with messaging, location and presence service, and which can link pseudonyms with their related identity information; a *mobile payment service provider* for users, allowing multiple payment procedures; a *client application*, that is a privacy agent in order to manage user pseudonyms and give support for notification and generation of location maps; and finally a *third party ticket application provider*, which provides location information according to the route information encoded in the ticket. Apart from the need to know the previous hash values, the key must be disclosed or correctly guessed in order to decode and even impersonate a message. But, when activating and using the tickets, all the previous used pseudonyms are also sent, then, the third party ticket application provider is able to trace all of these movements, and the network provider can even identify the user. Protection of pseudonyms is held only at the moment of the payment procedure.

Madlmayr et al. [33] propose a design and implementation of an e-ticketing system as an example of secure communication between web browsers and NFC targets, by using mobile phones and J2ME technology. A mobile phone is connected through NFC to a PC that acts as a proxy in order to connect to the Internet and download the ticket to the mobile device for its subsequent use. Firstly, during the ticket production, (1) a secure connection HTTPS is established between the PC browser and the ticket issuer; (2) the ticket is requested from the mobile phone through the PC browser; (3) the ticket is generated and signed by a TTP (control instance), (4) sent to the PC browser, and finally to

the mobile phone through NFC. All sent information in this ticket production is formatted in XML. During the ticket verification, (1) the reader sends the issuer identification to the mobile phone to identify the service, (2) the mobile phone sends all the available tickets for this service, (3) the reader selects the correct ticket for the event, and (4) the ticket is finally sent to the reader. In terms of privacy, anonymity is preserved for honest users, and they use PKI having each ticket and its issuer their own key pair. All the stored information is encrypted with the public key of their owners, and there is unlinkability between 2 tickets of the same mobile device. Although serial number of the mobile phone is neither used for authentication nor for identification processes, authentication of the mobile device is done by transferring its public key in order to encrypt the tickets. If this public key was stored in the control instance (TTP), tracking of the mobile device could be achievable for this static public key. In addition to these possible vulnerabilities, a plug-in must be installed in the mobile device in order to interact with the ticketing system, enabling then security risks if there was a malicious code.

Untraceable Heydt-Benjamin et al. [23] classify their proposal as an e-ticketing system, but the protocol is closer to an AFC system as the device is rechargeable and used as a wallet. The user receives a cookie when entering the system and then, when exiting, he sends this entry cookie, the price is calculated and paid, and the user finally receives a paid-state cookie. User and reader authentication, as well as session key creation between them is done by using Re-Encryption Authentication (authentication of a reader to a ticket), in order to let the generation of temporary delegation keys distributed to each reader (online system). By using this authentication protocol, the issuer signature can be decoded by the readers private keys, as they are delegated keys from the issuer and, this way, all the readers are authorized to interact with this information. The payment is done by using Chaum's electronic coins. The system is implemented as an hybrid system that allows mobile devices as well as contactless smart cards (through NFC), but it is proven that mobile devices offer greater degree of anonymity than smart cards. Anonymity for users is evaluated in each protocol transaction separately. User tracking is not possible as purchase and entering/exiting are not linked. The value of the ticket could be recharged but not linked neither with the user nor the previous *ticket id* (one-time identifiers).

Vives-Guasch et al. [53, 52] presented an electronic and secure automatic fare collection system which is adapted for massive users transport and preserves privacy for users. The proposal uses group signatures schemes in order to allow revocation of the identity of users in case of misbehaviour.The system, differently than previous proposals, does not require to obtain a new credential every time the user joins in the system in order to obtain untraceability. The authors have designed the AFC system in order to use the personal mobile devices of the users.

Considerations on the AFC systems In the majority of these schemes, the provider can link different journeys from the same user [57, 6, 24, 27, 33]. In a linkable system, the disclosure of the identity of the user in a journey leads to the disclosure of all the journeys of the same user (weak anonymity). So that, the provider knows where they go, when and the time of the journeys. The knowledge of users' behavior allows the creation of the users' profiles. The profiles are useful for the provider because they can be used to improve the transportation system or to define a commercial product specifically for one profile. Nonetheless, the creation of users' profiles is a serious violation of the privacy, i.e. the AFC system must avoid the tracking of the users. In [23] the provider can not trace these journeys, but then a new credential is needed for every journey, what means that there is an important extra cost in these mass-transport systems, where the entrances and exits of the system have to be as quick as possible. The credential renewal requires a more complex provider structure, i.e. costly, because it must manage a high number of credentials. Finally, if the users must take some time to obtain a new credential, they probably will not obtain the new credential loosing their privacy.

Related to the devices used in the proposals, the latest trends go in the direction to use mobile devices (e.g. mobile phones, PDAs, smart phones, etc.) [57, 23, 27, 33] for these systems, instead of smart cards [6, 23, 24]. Thus, we can say that the mobile device is a user's requirement in the AFC systems.

3.3 Information

In this section, we describe the information that is usually included in the entrance ticket in Table 7 and the information in the exit ticket in Table 8.

Entrance ticket	
Name	Description
Serial number	generated by $\mathcal{P}_S$
Entrance station	$\mathcal{P}_S$ identifier
Entrance timestamp	
Validity time	
Direction	journey direction

Table 7. Information in entrance ticket

Exit ticket	
Name	Description
Ticket serial number	sent by $\mathcal{U}$
Destination station	
Paid fare	

Table 8. Information in exit ticket

4 Conclusions and contributions

We have presented the advantages of electronic ticketing (ET) and automatic fare collection systems (AFC). We can buy, receive and validate the ET without neither need to move to a certain place to make these actions nor to print it. The paper costs reduction in addition to the improved processes are good arguments to adopt the ET. The AFC systems allows to reduce costs and it improves the control of the infrastructures; some examples could be the real-time traffic density monitorization and the management strategy of infrastructures depending on the passenger flows.

Nonetheless, we have presented the privacy threats to which users are exposed when they use ET and AFC. Anonymity of users is not always guaranteed (for honest users), so that appears the problem of ticket tracking, and the real possibility to link the ticket to a certain user. The privacy and the users identity could be revealed and all their entering and exiting movements in these systems could be also tracked. Next, we have classified and described the different approaches to address the problem of privacy for ET and AFC systems.

First proposals in ET do not consider the anonymity and the more recent proposals incorporate the revocable anonymity as a core property. Thus our work has focused on the revocable anonymity [8, 54] and we have included the exculpability as a new security requirement. The first work [8] was published in a national congress and one version improved with conflict resolution [54] has been published in one international congress. Actually, we are developing as a first prototype through using mobile devices for the users with Near-Field Communication contactless technology in order to evaluate its real usability, and we have incorporated the reusability property. We are planning to submit the work to an ISI JCR journal. At the same time, we have initiated the actions to apply for a patent for an ET protocol that we have developed for an ET project. Two companies participate in the project and are interested in our technology.

In the AFC systems, the provider can link different journeys from the same user in the majority of the schemes, or the user must obtain a new credential every new journey. We have proposed two AFC systems [53, 52] that offer strong privacy for honest users, and it is not necessary to obtain a new credentials for every journey. This system has been designed in order to use personal mobile devices. The first work [53] has been published in a national congress and an improved version [52] in an international congress. The system is currently being submitted to international journals. Our future work is to adapt the proposed system so that it can be used in the Vehicular Ad-hoc Networks (VANET).

We think that we have a slight delay according to the task schedule, and that we can obtain more and significative results. We are encouraged to continue our research in this line because several companies are interested in our protocols.

4.1 List of contributions

A list of papers published by members of the ARES group follows.

LNCS

1 Vives-Guasch, A.; Payeras-Capella, M.; Mut-Puigserver, M., Castell-Roca, J.; "E-Ticketing scheme for mobile devices with exculpability", *Data Privacy Management (DPM), Fifth International Workshop*, Lecture Notes in Computer Science, Springer Verlag, vol. 6514 , pp (to appear), 2010.

Conferences

2 Castell-Roca, J.; Vives-Guasch, A.; "Billetes electrnicos seguros", *Reunin Espaola sobre Criptologa y Seguridad de la Informacin (RECSI)*, pp. 379-387, ISBN 978-84-691-5158-7, 2008.

3 Vives-Guasch, A.; Castell-Roca, J.; Payeras-Capella, M.; Mut-Puigserver, M.; "Sistema de peajes electrnicos seguro con anonimato revocable", *Reunin Espaola sobre Criptologa y Seguridad de la Informacin (RECSI)*, pp. 201-205, ISBN 978-84-693-3304-4, 2010.

4 Vives-Guasch, A.; Castell-Roca, J.; Payeras-Capella, M.; Mut-Puigserver, M.; "An Electronic and Secure Automatic Fare Collection System with Revocable Anonymity for Users", The 8th International Conference on Advances in Mobile Computing & Multimedia (MoMM2010), ACM, (to appear), 2010.

References

1. AirCanada. Mobile check-in, 2007. http://www.aircanada.com/en/travelinfo/traveller/mobile/mci.html.
2. Amadeus and ACTE. Upwardly mobile: The next step for travel management, 2008. http://www.amadeus.com/documents/corporations/Upwardly
3. AMSBUS, 2008. http://www.svt.cz/en/amsbus/.
4. A. Arnab and A. Hutchison. Ticket based identity system for drm. *Proceedings Information Security South Africa*, 2006. Sandton, South Africa.
5. F. Bao. A scheme of digital ticket for personal trusted device. *15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC04)*, 4:3065–3069, 2004. IEEE.
6. Levente Buttyn, Tamas Holczer, and Istvn Vajda. Providing location privacy in automated fare collection systems. In *In Proceedings of the 15th IST Mobile and Wireless Communication Summit, Mykonos, Greece*, June 2006.
7. J. Caron, I. Lagrange, and L. Robet. Contactless cell phone payment and e-ticketing: Japan leads the way at cartes & identification 2007, 2007. CARTES 2007 Press release, http://www.cartes.com/ExposiumCms/cms_sites/SITE_324050/ressources324050/cp_japon_gb.pdf.
8. J. Castellà-Roca and A. Vives-Guasch. Billetes electrónicos seguros. *X RECSI, Reunión Española sobre Criptología y Seguridad de la Información*, pages 379–387, 2008. ISBN 978-84-691-5158-7.

9. C.C. Chang, C.C. Wu, and I.C. Lin. A secure e-coupon system for mobile users. *International Journal of Computer Science and Network Security*, 6(1):273–280, 2006. IEEE.
10. D. Chaum, A. Fiat, and M. Naor. Untraceable electronic cash. *CRYPTO'88: Proceedings on Advances in Cryptology*, pages 319–327, 1988. LNCS 403.
11. David Chaum. Blind signatures for untraceable payments. *Advances in Cryptology - CRYPTO'82*, pages 199–203, 1983.
12. Yu-Yi Chen, Chin-Ling Chen, and Jinn-Ke Jan. A mobile ticket system based on personal trusted device. *Wireless Personal Communications: An International Journal*, 40(4):569–578, 2007.
13. J. Elliot. The one-card trick multi-application smart card e-commerce prototypes. *Computing & Control Engineering Journal*, 10(3):121–128, 1999. IET.
14. CI. Fan and CL. Lei. Multi-recastable ticket schemes for electronic voting. *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, E81A(5):940–949, 1998.
15. K. Fujimura, H. Kuno, M. Terada, K. Matsuyama, Y. Mizuno, and J. Sekine. Digital-ticket-controlled digital ticket circulation. *8th USENIX Security Symposium*, pages 229–240, 1999. USENIX.
16. K. Fujimura and Y. Nakajima. General-purpose digital ticket framework. *3rd USENIX Workshop on Electronic Commerce*, pages 177–186, 1998. USENIX.
17. Ko Fujimura, Yoshiaki Nakajima, and Jun Sekine. Xml ticket: Generalized digital ticket definition language. *W3C XML-Dsig'99*, 1999.
18. FynBus. Sms-billet, 2007. http://www.fynbus.dk/.
19. N. Granados, K. Gupta, and R. Kauffman. It-enabled transparent electronic markets: the case of the air travel industry. *Inf. Syst. E-Business Management*, pages 65–91, 2007.
20. D. Haneberg. electronic ticketing a smartcard application case-study. Master's thesis, Institut Für Informatik, 2002. Technical Report 2002-16, http://www.informatik.uni-augsburg.de/lehrstuehle/swt/se/publications/2002-e_ticket_scard_app_stud/2002-e_ticket_scard_app_stud-pdf.pdf.
21. D. Haneberg. Electronic ticketing: risks in e-commerce applications. *Digital excellence*, pages 55–66, 2008. Springer-Verlag, ISBN 3540726209.
22. Dominik Haneberg, Kurt Stenzel, and Wolfgang Reif. Electronic-onboard-ticketing: Software challenges of an state-of-the-art m-commerce application. In K.Pousttchi and K.Turowski, editors, *Workshop Mobile Commerce*, volume 42 of *Lecture Notes in Informatics (LNI)*, pages 103–113. Gesellschaft für Informatik (GI), 2004.
23. Thomas S. Heydt-Benjamin, Hee-Jin Chae, Benessa Defend, and Kevin Fu. Privacy for public transportation. In *6th Workshop on Privacy Enhancing Technologies (PET 2006)*, pages 1–19, 2006. LNCS 4258.
24. Seng-Phil Hong and Sungmin Kang. Ensuring privacy in smartcard-based payment systems: A case study of public metro transit systems. In *Communications and Multimedia Security*, pages 206–215, 2006.
25. IATA. E-ticketing, 2007. http://www.iata.org/stbsupportportal/e-ticketing.htm.
26. IATA. Industry bids farewell to paper ticket, 2008. http://www.iata.org/pressroom/pr/2008-31-05-01.htm.
27. O. Jorns, O. Jung, and G. Quirchmayr. A privacy enhancing service architecture for ticket-based mobile applications. In *2nd International Conference on Availability, Reliability and Security*, pages 374–383, Vienna, Austria, Apr 2007. ARES 2007 - The International Dependability Conference. vol. 24.

28. H. Kreft. Cashing up with mobile money - the faircash way. *Euro mGov 2005*, page 29, 2005. Sussex University, Brighton (UK), Mobile Government Consortium International LLC,ISBN: 0-9763341-0-0.
29. K. Kuramitsu and K. Sakamura. Electronic tickets on contactless smartcard database. In *Proceedings of the 13th International Conference on Database and Expert Systems Applications*, pages 392–402, 2002. LNCS 2453.
30. Kimio Kuramitsu, Tadashi Murakami, Hajime Matsuda, and Ken Sakamura. Ttp: Secure acid transfer protocol for electronic ticket between personal tamper-proof devices. In *24th Annual International Computer Software and Applications Conference (COMPSAC2000)*, pages 87–92, Taipei, Taiwan, Oct 2000. vol. 24.
31. LeedsUnited. Official leeds sms, 2007. http://www.leedsunited.com/page/Welcome.
32. J. Lutgen. The security infrastructure of the german core application in public transportation. In *Isse/secure 2007 Securing Electronic Business processes: Highlights of the Information Security Solutions Europe/secure 2007 Conference*, pages 411–419, Vienna, Austria, 2007. Vieweg&Teubner Verlag, ISBN: 3834803464.
33. Gerald Madlmayr, Peter Kleebauer, Josef Langer, and Josef Scharinger. Secure communication between web browsers and nfc targets by the example of an e-ticketing system. In *EC-Web '08: Proceedings of the 9th international conference on E-Commerce and Web Technologies*, pages 1–10, Berlin, Heidelberg, 2008. Springer-Verlag.
34. M. Mambo, K. Usuda, and E. Okamoto. Proxy signature: Delegation of the power of sign messages. *IEICE Trans. Fundamentals*, E79-A(9):1338–1354, 1996.
35. M. Mambo, K. Usuda, and E. Okamoto. Proxy signatures for delegating signing operations. *Proceedings of 3rd ACM Conference on Computer and Communications Security (CCS'96)*, pages 48–57, 1996. ACM Press.
36. Antonio Mana, Jesús Martínez, Sonia Matamoros, and J.M. Troya. Gsm-ticket: Generic secure mobile ticketing service. *Gemplus World Developers Conference*, 2001. Gemplus, Paris (France).
37. S. Matsuo and W. Ogata. Electronic ticket scheme for its. *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, E86A(1):142–150, 2003.
38. R.L. McDaniel and F. Haendler. Advanced rf cards for fare collection. In *Commercial Applications and Dual-Use Technology, Conference Proceedings*, pages 31–35. Telesystems Conference, 1993.
39. F. Mihlberg. On the formal analysis of e-ticketing protocols. Master's thesis, School of Computer Science and Engineering, 2002.
40. T. Nakanishi, N. Haruna, and Y. Sugiyama. Unlinkable electronic coupon protocol with anonymity control. *Proceedings of the Second International Workshop on Information Security*, pages 37–46, 1999. LNCS 1729, ISBN: 3-540-66695-8.
41. NY.Times. Paper is out, cellphones are in, 2008. http://www.nytimes.com/2008/03/18/technology/18check.html.
42. B. Patel and J. Crowcroft. Ticket based service access for the mobile user. *Proceedings of the 3rd Annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM'97)*, pages 223–233, 1997. Budapest, Hungary.
43. F. Pedone. A two-phase highly-available protocol for online validation of e-tickets. *Hewlett-Packard Labs Technical Reports*, 2000. HPL-2000-116 20000929.
44. Prague.Public.Transport. Sms tickets for public transport in prague, 2007. http://www.prague.net/sms-ticket.
45. D. Quercia and S. Hailes. Motet: Mobile transactions using electronic tickets. In *1st International Conference on Security and Privacy for Emerging Areas in*

Communications Networks, Proceedings, pages 374–383, Athens, Greece, Sep 2005. vol. 24.

46. C. Serban, Y. Chen, W. Zhang, and N. Minsky. The concept of decentralized and secure electronic marketplace. *Electronic Commerce Research*, 8(1-2):79–101, 2008. ISSN: 1389-5753.
47. I.W. Siu and Z.S. Guo. The secure communication protocol for electronic ticket management system. In *8th Asia-Pacific Software Engineering Conference (APSEC2001)*. University of Macau, 2001.
48. W.I. Siu and Z.S. Guo. Application of electronic ticket to online trading with smart card technology. *Proceedings of the 6th INFORMS Conference on Information Systems and Technology (CIST-2001)*, pages 222–239, 2001. Miami Beach, Florida (US).
49. R. Song and L. Korba. Pay-tv system with strong privacy and non-repudiation protection. *IEEE Transactions on Consumer Electronics*, 49(2):408–413, 2003. ISBN 0-7695-1969-5/03.
50. Spanair. Spanair y vodafone españa presentan la tarjeta de embarque móvil, 2007. http://www.spanair.com/web/es-es/Sobre-Spanair/Noticias-y-eventos/Spanair-y-Vodafone-Espana-presentan-la-tarjeta-de-embarque-movil/.
51. M.E.G. Valdecasas-Vilanova, Regine Endsuleit, Jacques Calmet, and Interner Bericht. State of the art in electronic ticketing. Master's thesis, Institut für Algorithmen und Kognitive Systeme, 2003. ISSN: 1432-7864.
52. Arnau Vives-Guasch, Jordi Castell-Roca, Magdalena Payeras-Capella, and Mut-Puigserver. An electronic and secure automatic fare collection system with revocable anonymity for users. In *The 8th International Conference on Advances in Mobile Computing & Multimedia (MoMM2010)*, ACM, page (to appear), 2010.
53. Arnau Vives-Guasch, Jordi Castell-Roca, Magdalena Payeras-Capella, and Mut-Puigserver. Sistema de peajes electrnicos seguro con anonimato revocable. In *Reunin Espaola sobre Criptologa y Seguridad de la Informacin (RECSI)*, pages 201–205, 2010. ISBN 978-84-693-3304-4.
54. Arnau Vives-Guasch, Magdalena Payeras-Capella, Mut-Puigserver, and Jordi Castell-Roca. E-ticketing scheme for mobile devices with exculpability. In *Data Privacy Management (DPM), Fifth International Workshop*, volume 6514 of *Lecture Notes in Computer Science*, page (to appear), 2010. ISSN 0302-9743.
55. A. von Dörnberg. The global phenomenon of low cost carrier growth. *Trends and Issues in Global Tourism*, pages 53–59, 2007. Springer-Verlag Berlin and Heidelberg GmbH & Co. KG., ISBN-13: 9783540708315.
56. Guilin Wang, Feng Bao, Jianying Zhou, and R.H. Deng. Proxy signatures scheme with multiple original signers for wireless e-commerce applications. *Vehicular Technology Conference, VTC2004-Fall*, 5:3249–3253, 2004. IEEE.
57. Hua Wang, Jinli Cao, and Yanchuan Zhang. Ticket-based service access scheme for mobile users. *Aust. Comput. Sci. Commun.*, 24(1):285–292, 2002.
58. Shu-Cging Wang, Kuo-Qin Yan, and Chia-Hui Wei. Mobile target advertising for mobile user. *International Workshop on Business and Information (BAI 2004)*, V2, 2004. Taipei, Taiwan.