Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

A survey of electronic ticketing applied to transport

Macià Mut-Puigserver [a,*], M. Magdalena Payeras-Capellà [a], Josep-Lluís Ferrer-Gomila [a], Arnau Vives-Guasch [b], Jordi Castellà-Roca [b]

[a] Universitat de les Illes Balears, Departament de Ciències Matemàtiques i Informàtica, Carretera de Valldemossa, Km. 7.5, Palma, The Balearic Islands, Spain

[b] Universitat Rovira i Virgili, Departament d'Enginyeria Informàtica i Matemàtiques, UNESCO Chair in Data Privacy, Av. Països Catalans 26, Tarragona, Catalonia, Spain

ARTICLE INFO

Article history:
Received 27 January 2012
Received in revised form
8 May 2012
Accepted 10 July 2012

Keywords:
Electronic tickets
e-tickets
Privacy
Security
Anonymity
Cryptography

ABSTRACT

A wide variety of transport systems can benefit from the use of Electronic Ticketing (ET). ET systems are progressively introduced in transports systems, and produce a reduction of the associated economic costs and time intervals, and the control of the system is improved. However, the use of ET systems enables various privacy abuses both in real-time and retrospect since the anonymity of users is not always guaranteed and, therefore, users can be traced and their profiles of usual movements can be created. In our review article, we classify and describe the main proposals with special focus on the properties related to user privacy.

1. Introduction

The use of Information Technologies (IT) in the day-by-day operations is growing dramatically. Tourism is one of the most affected sectors by the use of IT. Nowadays, it is possible to get information easily about a certain destination, look for flights reaching any place, book a hotel room or even get museum or park tickets, for example. Besides, all these actions can be performed in a notably comfortable way: they can be done at home and there are not temporal restrictions.

Users of paper-based tickets have to move to the ticket issuer entity in order to receive it, causing loss of time, or managing a device that could print the ticket. For example, an executive that is moving to the airport by taxi could be able to buy the ticket by using his mobile phone, but the ticket cannot be easily printed in this scenario. These limitations require to move to the issue agency, or alternatively to buy the ticket in another place. Paper ticket management has costs for users and companies, which could be reduced. Actually, the costs of a paper ticket issuing is low, but there is a great amount of issued tickets, so that it becomes a cost to be taken into account. Managing costs have to be taken into consideration.

The degree of importance of these changes depends on the use of IT held by the companies. In general, the use of IT is heterogeneous due to differences between sectors and also between every company's potential. Great companies prefer to exploit IT in order to get more performance by using the latest technological advances. Otherwise, little companies invest less in IT. In the case of little interrelated companies, the use of IT depends on the use that these little companies could make.

The use of electronic tickets in a company affects the business itself and also the user. Purchase and reception

* *Corresponding author*. Tel.: +34 971 17 32 46; fax: +34 971 17 30 03.
E-mail address: macia.mut@uib.es (M. Mut-Puigserver).
0167-4048/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.cose.2012.07.004

phases could be totally electronic, but it requires that the validation process must be also electronic. Users carry tickets while they are moving, and validate them in order to get access to the service. For this reason, the user must have a suitable device in order to manage and use electronic tickets. Mobile devices (mobile phones, PDAs or Smart phones) are considered the best positioned devices in these electronic ticketing systems. These devices offer suitable computation and storing capacities and a rich variety in the latest wireless communication technologies (Bluetooth, NFC and also Wi-Fi). All these features are available in a reduced size, providing mobility and flexibility for these systems.

In addition to the previous considerations, the real application of these electronic ticketing systems depends on their security, due to the ease of copy of electronic contents and privacy issues. Electronic tickets must be equally or even more secure than paper tickets.

Transport is one of the main sectors that use tickets in their standard activity. Paper tickets are being progressively substituted for electronic tickets, reducing then paper costs and making all the process more dynamic.

Electronic tickets can be used for multiple transport services. In this way, the AMSBUS (2008) booking system from the Czech Republic allows the purchase of SMS tickets. First, the passenger receives the ticket into his mobile phone. Then, 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 (2007).

Flight companies are world leaders in the use of electronic tickets and emerging IT. The International Air Transport Association (IATA) started in 2004 a programme to introduce the use of electronic tickets (IATA, 2007) which was totally implemented in 2008. This initiative eliminates costs of ticket printers, maintenance, and ticket distribution and represents 3 billion US dollar annual savings due to the fact that an e-ticket costs 1US dollar to process versus 10 US dollar per paper ticket (IATA, 2008)

Another example of that could be the electronic air flight boarding pass. Vodafone and Spanair (Spanair, 2007) made a test in 2007 where passengers received their electronic boarding passes into their mobile phones. Other companies like Air Canada (AirCanada, 2007) or Continental (NY.Times, 2008) have followed the same direction and they offer similar services to their customers.

These examples prove two important facts: (i) there is a progressive introduction of electronic tickets in different kinds of services; and (ii) mobile phones are the main platform for e-tickets.

We next enumerate some advantages of the use of electronic tickets on mobile phones:

- Customers are able to book everywhere, even without a printer.
- Tickets can be bought and used immediately.
- Easier and faster communication between the customers and the company.
- Company saves resources and speeds up the management process.

Finally, although transport is the most representative scenario of e-ticketing use, electronic tickets can also be used in other fields. Leisure sector has some examples of e-ticketing systems that are being applied. They can be used to book sport events or any other kind of live show. For instance, LeedsUnited (2007) supporters can book a match and later receive an SMS with the booking confirmation together with some added information such as their assigned seats.

1.1. *Electronic ticket: definition*

The ticket is a contract between a user and a service provider. If the user demonstrates his ownership of the ticket, he obtains the right to use the service under its terms and conditions (Fujimura and Nakajima, 1998) (e.g., ticket validity time). Commonly, the ticket validation is required in order to use the service. Depending on the conditions of the ticket, it can be validated once, a predefined several times or indefinitely until a deadline.

The ticket must include elements to assure the system's security and the users' privacy. The requirements related to security and privacy can vary among different applications of e-tickets. In some cases, security would be critical, such as e-ticket falsification on air travel. In others, privacy requirements, as the anonymity of the users, are mandatory.

1.2. *Objectives*

The main purpose of this survey is to construct specified knowledge in electronic ticketing systems by firstly defining their main security requirements, their phases, describing the involved participants in these systems, also defining the information stored into the ticket, and finally a survey of the latter in electronic ticketing proposals.

This work is going to be useful to go beyond future research based on e-ticketing systems. These systems have achieved worldwide renown and public transport can surely benefit from these technological advances due to the improvement of both the security aspects presented in recent works and of the verification speed achieved with new portable devices.

1.3. *Document organization*

First, a description of electronic ticketing systems is made by defining the different participants that take part in these systems and identifying the phases involved in the use of tickets (Section 2). Next, the multiple services that can benefit of the use of electronic ticketing systems are exposed (Section 2.3). The information included in e-tickets is defined in Section 2.4. The general e-ticket requirements are described in Section 3 focussing specially in the security requirements.

A survey of the existing electronic ticketing proposals is made in Section 4, by classifying these proposals depending on an essential feature: the privacy provided by the schemes, so anonymity is a key factor in this section. As a result, Section 4.1 shows the anonymous proposals, Section 4.2 shows the full-revocable anonymous proposals, Section 4.3 shows the selective-revocable anonymous proposals and, finally, Section 4.4 shows non-anonymous proposals.

2. Electronic tickets

This section includes the analysis of the e-ticketing systems, first defining the involved participants, the related phases, the most suitable services related to public transport of these systems and the information to be included in the e-tickets.

2.1. Actors

We introduce the participants who are involved in an electronic ticketing system, according to the authors of (Fujimura et al., 1999a, 1999b; Mana et al., 2001; Mihlberg, 2002; Matsuo and Ogata, 2003; Quercia and Hailes, 2005):

- 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. E-tickets can be issued by both service providers and intermediaries (Siu and Guo, 2001b).
- Service provider: receives the e-ticket from the user and validates it. If correct, then it provides access to the service to the user.

These are the general and main participants in e-ticketing systems, but some systems include other participants. For example, a *shop* or a *broker* (Fujimura et al., 1999a, 1999b; Kuramitsu and Sakamura, 2002; Wang et al., 2004a). Moreover, if public key cryptography systems (Patel and Crowcroft, 1997; Serban et al., 2008) are used, a *Certification Authority* (CA) is also included. In some cases, (Siu and Guo, 2001a), the e-ticketing system is based on the use of Smart-Cards, so the *Smart-Card issuer* is also included in the system. The scheme presented in Chen et al. (2007) includes a *user agent* and the *network access service provider*. The system proposed in Jorns et al. (2007) 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 trusted participant. Other systems also consider the possibility to pay for the e-ticket, so that the *payment service provider*, the *bank* and the *credit card issuer* are also participants involved in the system.

2.2. Phases

According to most authors, an electronic ticket system consists of three main phases: *e-ticket payment*, *issue* and *validation* (Elliot, 1999; Fujimura et al., 1999a; Siu and Guo, 2001a; Siu and Guo, 2001b; Kuramitsu and Sakamura, 2002; Matsuo and Ogata, 2003; Bao, 2004; Quercia and Hailes, 2005; Chen et al., 2007). However, these three phases are not unanimously defined. Some authors (Patel and Crowcroft, 1997; Pedone, 2000; Mana et al., 2001; Mihlberg, 2002) group payment and issue phases, converting from three to two e-ticket phases: e-ticket issue and validation. Other proposals

Table 1 – Services for electronic ticketing systems.

Services	Air travel	Rail	Bus	Subway	Taxi	Tolls	No transport
(McDaniel and Haendler, 1993)						✓	
(Patel and Crowcroft, 1997)		✓	✓	✓			✓
(Elliot, 1999)		✓	✓	✓			
(Kuramitsu et al., 2000)							✓
(Kuramitsu and Sakamura, 2002)							✓
(Haneberg, 2002)		✓					
(Matsuo and Ogata, 2003)						✓	
(Valdecasas-Vilanova et al., 2003)		✓		✓		✓	
(Bao, 2004)	✓						✓
(Wang et al., 2004a)	✓						
(Haneberg et al., 2004)		✓					
(Heydt-Benjamin et al., 2006)		✓	✓	✓			
(Granados et al., 2007)	✓						
(Spanair, 2007)	✓						
(AirCanada, 2007)	✓						
(Prague. Public.Transport, 2007)			✓				
(FynBus, 2007)			✓				
(Jorns et al., 2007)		✓					
(Lutgen, 2007)		✓	✓	✓		✓	
(Caron et al., 2007)	✓	✓	✓	✓	✓	✓	✓
(LeedsUnited, 2007)							✓
(von Dörnberg, 2007)	✓						
(NY.Times, 2008)	✓						
(AMBUS, 2008)			✓				
(Haneberg, 2008)		✓					
(Serban et al., 2008)	✓						
(Bald et al., 2010)			✓				✓
(Kuntze and Schmidt, 2007)							✓
(Amoli et al., 2010)							✓
Total	9	10	9	6	1	5	9

(Wang et al., 2004b; Arnab and Hutchison, 2006; Chang et al., 2006) add a previous registration phase where users must be identified and authenticated in order to give them permission to use the service. In Heydt-Benjamin et al. (2006), as well as the previous phases, service *start* and *end* are considered. This real disagreement in electronic ticket phases is due to the great number of types of services where e-tickets can be used (Fujimura and Nakajima, 1998; Bao, 2004).

2.3. Services

The existing proposals have been evaluated depending on the services that can 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 (Patel and Crowcroft, 1997; Elliot, 1999; Haneberg, 2002, 2008; Valdecasas-Vilanova et al., 2003; Haneberg et al., 2004; Heydt-Benjamin et al., 2006; Jorns et al., 2007; Caron et al., 2007; Lutgen, 2007), followed by air travel (Bao, 2004; Wang et al., 2004a; Granados et al., 2007; Spanair, 2007; AirCanada, 2007; Caron et al., 2007; von Dörnberg, 2007; Serban et al., 2008; NY.Times, 2008), bus transport (Patel and Crowcroft, 1997; Elliot, 1999; Heydt-Benjamin et al., 2006; Prague. Public.Transport, 2007; FynBus, 2007; Caron et al., 2007; Lutgen, 2007, AMBUS, 2008) and subway (Patel and Crowcroft, 1997; Elliot, 1999; Valdecasas-Vilanova et al., 2003; Heydt-Benjamin et al., 2006; Caron et al., 2007; Lutgen, 2007), with one solely proposal used for taxi transport (Caron et al., 2007). Due to this predominance of transport services we have decided to focus this paper in transport e-ticketing systems. In 2006 in Germany, more than 25 e-ticketing projects were intended or in testing phases for public transport (Haneberg, 2008), most of them thought for short distance journeys.

We can find running systems applied to tolls (McDaniel and Haendler, 1993; Matsuo and Ogata, 2003; Valdecasas-Vilanova et al., 2003; Caron et al., 2007; Lutgen, 2007) but these are closer to electronic payment systems than electronic ticketing systems. Users pay for the service when they have used it depending on some usage factor and charging the amount of money directly to the current or credit card accounts. This kind of services can be implemented using Automatic Fare Collection systems (AFC). A similar payment system using e-tickets is applied to Location Based Services in (Amoli et al., 2010). Also a generic ET system is used in (Kuntze and Schmidt, 2007) as a method of service access control in a Trusted Computing environment. The rest of the proposals are not related to transport, instead, they are oriented to the leisure sector (Patel and Crowcroft, 1997; Kuramitsu et al., 2000; Kuramitsu and Sakamura, 2002; Bao, 2004; LeedsUnited, 2007; Caron et al., 2007; Bald et al., 2010), as sports or cultural events.

2.4. Information

Like paper tickets, electronic tickets must include some basic information for their practical use. In this section, information fields that electronic tickets can include are briefly described:

- Serial number (SN): unique identification of every e-ticket.
- Issuer (IS): entity who is responsible for issuing the e-ticket. This issuer can also be the service provider or an intermediary.
- Service provider (SP): entity who offers the service to the user.
- User (US): information about the e-ticket owner. In case of existence of this field in the e-ticket, user anonymity could not be achieved.
- Service (SV): description of the service contract.
- Terms and conditions (TC): definition of the e-ticket terms and conditions, or alternatively an external link to enable consultation.
- Type of e-ticket (TT): e-ticket includes a field describing its type.
  - Transferability (TF): if this field is permitted, transferability to another user is allowed.
  - Number of uses (NU): information about the allowed number of e-ticket uses.
- Destination (DT): this field is used for transport services in order to have user destination information.
- Attributes (AT): other attributes of the e-ticket that depend on the service (e.g., theatre seat).
- Validity time (VT): it includes two timestamps, the starting and the expiration dates.
- Date of issue (DI): 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 (DS): e-ticket issuer has a public key cryptosystem key pair, being able to digitally sign the e-ticket.
- Device identification (DV): e-ticket is linked to a specific device.

3. E-tickets requirements

We can classify e-ticket requirements into two categories. On the one hand, we have security requirements, and on the other hand we have functional requirements for e-tickets. Some of them are difficult to classify because they can have an impact in both categories: functionality and security.

In this paper we list all security requirements found in previous references, and most important functional requirements. Authors tend to cite those requirements that will be accomplished by the provided solution, and here we haver tried to be comprehensive. Nevertheless, not all the following requirements have to be met in all environments. It is well-known that security and efficiency, e.g., are conflicting objectives. So, scenarios will determine which requirements are more important in every case. We have included cites in each requirement, the number of which can be an indicator (not infallible) on their importance. We omit cites referred to anonymity (a very important requirement), because we delve into the subject in following section.

3.1. Security requirements

- **Definition 1 (Integrity, IT)** (Fujimura and Nakajima, 1998; Pedone, 2000; Siu and Guo, 2001a; Siu and Guo, 2001b; Vives-

Guasch et al., 2012; Wang et al., 2004a). It has to be possible to verify if the content of the e-ticket has been modified, as regards the one issued by the correspondent authorized issuer.

All the participants have to be able to verify if an e-ticket has been manipulated, that is to say, the e-ticket has to be issued by the issuer. In the electronic world, it is relatively easy to achieve this requirement, but in the paper world, it can be sometimes very easy to manipulate a paper ticket.

- **Definition 2 (Authenticity, ATH)** (Bao, 2004; Jorns et al., 2007; Patel and Crowcroft, 1997; Pedone, 2000; Siu and Guo, 2001a; Siu and Guo, 2001b; Vives-Guasch et al., 2010; Vives-Guasch et al., 2012; Wang et al., 2004a). A user has to be able to verify who has issued an e-ticket.

The fulfilment of this requirement will help users to verify if the issuer is an authorized one.

- **Definition 3 (Non repudiation of origin, NRO)** (Chen et al., 2007; Quercia and Hailes, 2005; Siu and Guo, 2001a; Siu and Guo, 2001b; Vives-Guasch et al., 2010; Vives-Guasch et al., 2012; Wang et al., 2004a). The user that has sent or generated a message does not have to be able to deny that she has sent or generated it.

This requirement can be useful in several stages, but it is particularly important related to a valid issued e-ticket: the issuer has not to be able to deny having issued that e-ticket, and with a specific content. Observe that, in fact, this requirement comprehends authenticity and integrity requirements: if the user cannot deny having issued an e-ticket it means that it can be verified he has issued the e-ticket (authenticity) and that nobody has modified the content of the e-ticket (integrity). Sometimes it will be necessary that a user that has requested an e-ticket issue, not to be able to deny this request (specially if there is a payment for the e-ticket, and even if this e-ticket is a present).

- **Definition 4 (Non repudiation of receipt, NRR)** (Haneberg et al., 2004; Quercia and Hailes, 2005; Siu and Guo, 2001b). A user receiving a message has not to be able to deny after the fact having received it.

This requirement, also, can be useful in several stages. For instance, a user that has requested and received an e-ticket has not to be able to deny having received it; or a provider that has received an e-ticket for a service, should not be able to deny having received that e-ticket.

- **Definition 5 (Unforgeability, UNF)** (Bao, 2004; Chen et al., 2007; Fujimura and Nakajima, 1998; Haneberg et al., 2004; Matsuo and Ogata, 2003; Mana et al., 2001; Patel and Crowcroft, 1997; Siu and Guo, 2001a; Siu and Guo, 2001b; Vives-Guasch et al., 2012). Only authorized users can issue valid e-tickets.

In other words, it has not to be possible to forge e-tickets to be given in good, as if they were issued by an authorized issuer. This requirement is directly related with non-repudiation of origin requirement, and therefore with integrity and authenticity requirements.

- **Definition 6 (Fairness, FR)** (Chen et al., 2007; Vives-Guasch et al., 2012). At the end of an exchange between two or more parties or every part can achieve the expected items or none of the parts can stand in a privileged situation.
  This requirement is closely related to non-repudiation, but goes a step further because it does not only seek to ensure that the parties cannot deny having participated in a transaction a posteriori, but also that the parties are committed, in relation to a particular exchange, with fairness: or everybody or nobody. This requirement can be useful for multiple processes related to e-tickets management:
  - issue: if the costumer pays the amount of the e-ticket is worth, then she should receive a valid e-ticket from the issuer, and vice versa, if the customer receives a valid e-ticket, she has to pay the corresponding amount or she must provide a proof that she has received the e-ticket. We can think of some exceptions: donations (between users), free e-tickets (for some events), etc.
  - use: if the client delivers a valid e-ticket to the service provider, the service provider must provide the service linked to the e-ticket, and vice versa.
  - compensation: if the service provider has a valid e-ticket (received from a client) must receive, if applicable, the corresponding compensation (typically economic), and if the service provider has received such compensation, then she must provide a proof that she has received it (to prevent from claiming a collection in duplicate).

Therefore, a protocol will have to be designed to achieve the aforementioned properties. We are in front of a kind of fair exchange of values (an e-ticket for a payment, a service for an e-ticket), and so, some of the following properties will have to be met: fairness, abuse-freeness, timeliness, verifiability of the TTP, etc. It's out of the scope of this survey to explain the properties that can be found, for instance, in (Ferrer-Gomilla et al., 2010).

- **Definition 7 (Non-overspending, NOV)** (Bao, 2004; Fujimura et al., 1999a; Fujimura et al., 1999b; Haneberg et al., 2004; Matsuo and Ogata, 2003; Mana et al., 2001; Patel and Crowcroft, 1997; Pedone, 2000; Quercia and Hailes, 2005; Siu and Guo, 2001a; Siu and Guo, 2001b; Vives-Guasch et al., 2010; Vives-Guasch et al., 2012). E-tickets can only be used as agreed between the issuer and the user.

Non-reusable e-tickets cannot be reused after they have been spent. Reusable e-tickets can be used exactly the number of times agreed in the moment of issue. Finally, some e-tickets cannot be used after their valid period of time. Period and usable times can be combined in the same e-ticket (see reusability requirement). Mechanisms to control overspending can affect the anonymity requirement. Overspending can be prevented or detected. If overspending is detected in the

verification phase, it will not be allowed. If it is detected afterwards, some way to identify the overspender or possible overspenders will be necessary.

This requirement is closely related with the uniqueness requirement of paper-based tickets: they are unique documents. It means we can distinguish between the original and the copy (although some copies are difficult to identify). At least, in those cases where it is not easy to make a copy, system security is based on the fact that to falsify or duplicate tickets is difficult. Note that, here another requirement is related with uniqueness: forgery.

In the electronic world it is, perhaps, a nonsense to speak of original and copy: two identical strings of bits cannot be distinguished. Any accessible electronic document can be duplicated so many times as desired. When we want to talk about non-usable copies of electronic documents we have to use some technique in order to achieve this requirement:

a) tamper-resistant devices (e.g., Smart-Cards), prevent a document stored in that device to be manipulable, so the distribution of these unique documents will be possible among this kind of devices. But we have to deal with the problem that these devices are not widely available, and security is based on the fact that manipulation cost has to be higher than benefits that an attacker can obtain. When the value of the information stored in the device is high, and even when it is lower but accumulating transactions (from one ore more devices), the value can be high, these devices are not a good solution. Furthermore, the cost of the device and usability/commodity for users have to be considered.
b) Some entity keeps track of the used e-tickets in a centralized way, and so the uniqueness of the document is not guaranteed, but the uniqueness of the use can be guaranteed. What matters is the information on the central register. As regards to the moment the controller entity knows that an over-spending occurs, we can distinguish two types of techniques: prevention (the attempt of over-spending is detected and not allowed, typically with online transactions with that entity) and detection a posteriori (a case of over-spending is detected at a phase of the protocol, but after the fact that typically trying not to stand online transactions with the controller entity, but assuming a possible fraud).

Whatever the technique used, as we have said previously, it should only be able to use one valid copy of an e-ticket.

- **Definition 8 (Identified e-tickets, IDF)**. Identity of the proprietary of the e-ticket has to be verifiable.

Not all the paper-tickets present the same requirements with regard to anonymity, so we have to distinguish some possible scenarios for e-tickets. The first type are non-anonymous e-tickets, where the service requires user identification and authentication. It means that user identity has to be embedded in the e-ticket in some way, so that the service provider could verify that the user is authorized to spend that e-ticket. It is the case of plane e-tickets. In the boarding phase, the auxiliary people of the Air Company have to be able to verify that the flyer identity is the same as the identity contained in the e-ticket.

- **Definition 9 (Full-Revocable Anonymity, F-RAN)**. Anonymity of users can be revoked.

Identity of users are embedded, in some way (pseudonyms, real identity), in e-tickets. Typically, only a reduced subset of actors can reveal this identity, and generally, it will be done when overspending is detected during the verification process. It means that the same e-ticket could be used more times than desired. For identified e-tickets, this is not a problem: we know the identity of the overspender and so, appropriate actions can be undertaken. For anonymous e-tickets, anonymity has to be revocable in order to identify the overspender. Obviously, honest users should remain anonymous or, at least, they should be able to prove they are honest users.

- **Definition 10 (Selective-Revocable Anonymity, S-RAN)**. The identity of a fraudulent user of an a priori anonymous e-ticket can be revealed.

This requirement is quite similar to the previous one, but it is more restrictive: only dishonest users may lose anonymity. From a privacy point of view, this requirement is better than the previous one, and even it can be better than the next one. The problem is that it may require more complex technical solutions.

- **Definition 11 (Anonymous e-tickets, AN)**. A user of an e-ticket has to remain anonymous.

Some paper tickets allow users to remain anonymous in front of the issuer, verifier and service provider. Therefore e-tickets will have to maintain the requirement. This requirement deals with the way of of issuing and the way of spending the e-ticket. The anonymity remains during the life cycle of the e-ticket. However, depending on the kind of payment method used, the user could be identified in this phase. But, in any case, the user has to be able to spend the e-ticket without any kind of identification. Even colluded issuers and service providers should not be able to break anonymity of consumers. Some kind of e-tickets have to be anonymous, and in no case should be possible to know the identity of the user, even if it is known that somebody is trying or has tried to overspend the e-ticket.

- **Definition 12 (Exculpability, EXC)** (Vives-Guasch et al., 2010; Vives-Guasch et al., 2012). The service provider cannot falsely accuse an honest user of e-ticket overspending, and the user is able to demonstrate that he has already validated the e-ticket before using it.

This requirement was proposed recently in Vives-Guasch et al. (2012), for e-tickets. An honest user has to be able to prove that he has validated the e-ticket, and therefore the service provider cannot falsely accused him.

On the other hand, we have claimed that after an over-spending is detected the provider has to be able to identify the

overspender or possible overspenders. If the technical solution identifies the overspender there is no problem. Nonetheless, if the technical solution does not identifies the possible overspenders, it is mandatory that honest users can prove that they have used e-ticket accordingly the issuing conditions, i.e. they can no be accused of overspending. Perhaps it will suppose to lose anonymity and therefore these are not the best kind of solutions.

- **Definition 13 (Reusability, REU)** (Bao, 2004; Vives-Guasch et al., 2010; Vives-Guasch et al., 2012). The e-ticket can be used more than once.

An e-ticket could be used once (non-reusable, only can be spent once) or many times (reusable). In both cases, e-ticket overspending has to be prevented or detected. E-tickets can be used more than once as is the case of some urban transport, where a transport pass can be used for several travels (and a counter is decreased in every travel) or it can be used over a period of time. Even in some cases, the same e-ticket can be used in different services (for instance, bus and underground in the same city). E-tickets have to incorporate security measures that allow using the e-ticket in the valid period of time or for the number of uses agreed (or a combination of both, time and uses). Some authors name divisibility to this requirement (probably influenced by the similarities between e-ticket and e-money).

- **Definition 14 (Transferability, TF)** (Bao, 2004; Fujimura et al., 1999a; Fujimura and Nakajima, 1998; Jorns et al., 2007; Patel and Crowcroft, 1997; Quercia and Hailes, 2005; Siu and Guo, 2001a; Siu and Guo, 2001b; Vives-Guasch et al., 2012). One user can transfer her e-ticket to other users.

Some paper tickets can be transferred to other people (e.g., spectacle tickets, bus tickets). Obviously it is not the case of identified e-tickets (e.g., plane e-tickets). People receiving an e-ticket in a transfer (not directly from an authorized issuer) has to be able to verify that this e-ticket is valid (it will be easy if non-repudiation, integrity and authenticity are met) and not spent by the transferor entity (or previous transferors). When we are in front of gifts or donations between confident people (e.g., a friend, familiar) no special measures have to be taken, it is a personal matter if afterwards an overspending occurs.

But perhaps e-tickets can be resold, or e-tickets (spectacle entrances) can be a present from a third company (in exchange of buying some product from this company). The receiving entity has to be sure that the e-ticket is valid and not spent. But it's possible that the transferring user will try to overspend the e-ticket, and the transferor entity has to be able to prove she has not re-used the e-ticket. This problem should be specially handled when anonymity is revocable. Transferability will make necessary, sometimes, the fairness requirement.

Given the previous explanation, two additional definitions of transferability must be provided.

- **Definition 15 (Weak-Transferability, W-TF)**. The e-ticket is transferable but overspending cannot be verified in the transfer phase.

It means that the e-ticket can be used by a user different from the first proprietary of the e-ticket, but the receiver of the e-ticket will not be able to verify if that e-ticket has been provided to multiple users or if it has been used previously, when he receives the e-ticket. When using the e-ticket the user will know if it is valid (and perhaps it can be too late): the provider will inform her if the e-ticket had been used or not. This drawback can be softened if the recipient is provided some evidence of misuse of the transferor.

- **Definition 16 (Strong-Transferability, S-TF)**. The e-ticket is transferable and the receiver can verify that it is a valid e-ticket.

It means that the receiver has the warranty that only she will be able to use the e-ticket: the e-ticket has not been spent, and the originator will not be able to transfer the same e-ticket to other users.

3.2. *Functional requirements for e-tickets*

There are some other requirements that are not so directly related to security, but they can be as important as those explained previously.

- **Definition 17 (Expiry date, EXD)** (Siu and Guo, 2001b; Vives-Guasch et al., 2010; Vives-Guasch et al., 2012). An e-ticket is only valid during a time interval.

The fulfilment of this requirement can be useful in order to limit the size of databases containing information of used e-tickets.

- **Definition 18 (Offline verification, OFF)** (Bao, 2004; Chen et al., 2007; Fujimura and Nakajima, 1998; Haneberg et al., 2004; Matsuo and Ogata, 2003; Mana et al., 2001; Patel and Crowcroft, 1997; Pedone, 2000; Quercia and Hailes, 2005; Siu and Guo, 2001a; Vives-Guasch et al., 2010; Vives-Guasch et al., 2012). E-ticket verification can be done without any external connection.

In some scenarios, it will not be possible to contact with external databases or Trusted Third Parties, to verify if an e-ticket is valid or not. Perhaps, it will not be the general case, but a solution for this problem has to be thought. This requirement is much related to security mechanisms adopted.

- **Definition 19 (Online verification, ON)** (Bao, 2004; Matsuo and Ogata, 2003; Patel and Crowcroft, 1997; Pedone, 2000; Vives-Guasch et al., 2010; Vives-Guasch et al., 2012). E-ticket verification requires a persistent connection with a trusted centralized system.

Typically, the offline option is preferred, alleging costs or possible bottleneck, for example. However in an e-world where millions of transactions with credit card are made online (with "heavy" SSL connections), and with companies working with great computational power (e.g., Google, Facebook), it seems that this argument is no longer valid. In terms

of security, online verification is better for overspending checking.

- **Definition 20 (Portablity, PT)** (Chen et al., 2007; Fujimura and Nakajima, 1998; Mana et al., 2001; Siu and Guo, 2001b; Vives-Guasch et al., 2012). E-tickets must be capable of being stored on mobile devices.

E-tickets, as paper tickets, have to be portable by users. So, it has not to be necessary a laptop or a personal computer to handle e-tickets. For instance, mobile phones or smart cards will have to be able to store and process e-tickets.

- **Definition 21 (Reduced size, RS)** (Mana et al., 2001; Patel and Crowcroft, 1997; Vives-Guasch et al., 2012). E-tickets must be as short as possible.

Typically, e-tickets will be stored in mobile devices (e.g., a mobile terminal as a mobile phone or a smart card), and sometimes these devices will have a limited memory. Therefore, e-tickets have to be reduced in size as possible.

- **Definition 22 (Flexibility, FX)** (Jorns et al., 2007; Mana et al., 2001; Patel and Crowcroft, 1997; Quercia and Hailes, 2005; Vives-Guasch et al., 2012). E-tickets can be used in multiple environments.

We can think of a lot of different tickets (e.g., plane tickets, bus tickets, concert tickets, museum tickets). We can design a specific e-ticket for each application or we can adapt a general e-ticket for each application. Obviously, the latter solution is preferred in order to economize the solution, and to allow a better security analysis.

- **Definition 23 (Ease of use, EU)** (Fujimura et al., 1999a; Fujimura and Nakajima, 1998; Haneberg et al., 2004; Mana et al., 2001; Patel and Crowcroft, 1997; Vives-Guasch et al., 2012). Learning how to use e-tickets has to be easy.

We are thinking about e-ticketing as a solution for general public (using paper tickets nowadays, and not necessary especially confident in electronic means). E-tickets have to be so easy to use as paper tickets, and without new problems for users.

- **Definition 24 (Efficiency, EFF)** (Chen et al., 2007; Fujimura et al., 1999b; Jorns et al., 2007; Matsuo and Ogata, 2003; Mana et al., 2001; Patel and Crowcroft, 1997; Pedone, 2000; Vives-Guasch et al., 2010; Vives-Guasch et al., 2012). Processing an e-ticket has not to be resources consuming.

We can think efficiency from two points of view. First, mobile terminals can be limited in terms of computational power, and so protocol operations and especially cryptographic operations have to be reduced only to necessary ones. Second, communication capacity can also be limited, and so protocol has to be designed with this constrain in mind. Any, delay due to verification of validity of e-ticket has to be reasonable to be a valid solution for ticketing by electronic means.

- **Definition 25 (Payment openness, PYO)** (Fujimura and Nakajima, 1998; Mana et al., 2001; Vives-Guasch et al., 2012). E-tickets should be paid by usual payment systems.

The design of an e-ticket system has to bear in mind that sometimes it will be necessary a payment system to obtain the e-ticket. So, an e-ticket system has to allow different payment systems to be used in order to pay for the e-ticket (if necessary).

- **Definition 26 (Globally spendable, GS)** (Quercia and Hailes, 2005; Vives-Guasch et al., 2012). Costumers should be able to spend their e-tickets at any appropriate service provider.

This property is opposed to specific spendable e-tickets. In this case e-tickets can be used only at a specific provider.

- **Definition 27 (Availability, AV)** (Mana et al., 2001; Pedone, 2000; Vives-Guasch et al., 2012). E-tickets should be usable when needed.

This requirement can be seen as a security requirement, but it is quite difficult to address this problem only as a security one. We are thinking in denial of service attacks (difficult to handle), disaster events (more difficult to handle) or temporal malfunction of infrastructure (for instance, a power failure). This can mean that e-tickets cannot be verified, and sometimes the event cannot be delayed (e.g., a concert, a plane). A procedure to handle these situations has to be designed.

4. Existing security proposals

In this section we classify the ET proposals focussing in their privacy. In an ET system, anonymity is the closest related property to the user's privacy, since this property deals with the secrecy of the user identity and it guarantees that the user will not be identified.

According to the definition of anonymous tickets given in the previous section, we cannot consider as anonymous the tickets the proposals that intend to preserve the users' privacy by a policy-based approach. This approach consists in specifying a set of rules which define how information (in particular the user's identity) is stored and used. In addition, the rules show when and in what conditions this data can be revealed. We cannot survey the policy-based approach as a valid technique for anonymous tickets because users will not be able to spend the ticket without being identified; at the most, users should expect that ticket issuers or service providers do not reveal the users' identities. So, cryptographic protocol techniques are used in the e-ticketing schemes so as to assure the user's anonymity.

Below, in the following sections, the studied proposals have been classified depending on the anonymity compliance and according to the given definitions in Section 3 (definitions 8, 9, 10 and 11) as Fig. 1 shows. Firstly, in Section 4.1, anonymity-compliant schemes are described. The schemes that comply with anonymity but enable user identification disclosure are described in Section 4.2. Then, in Section 4.3, we

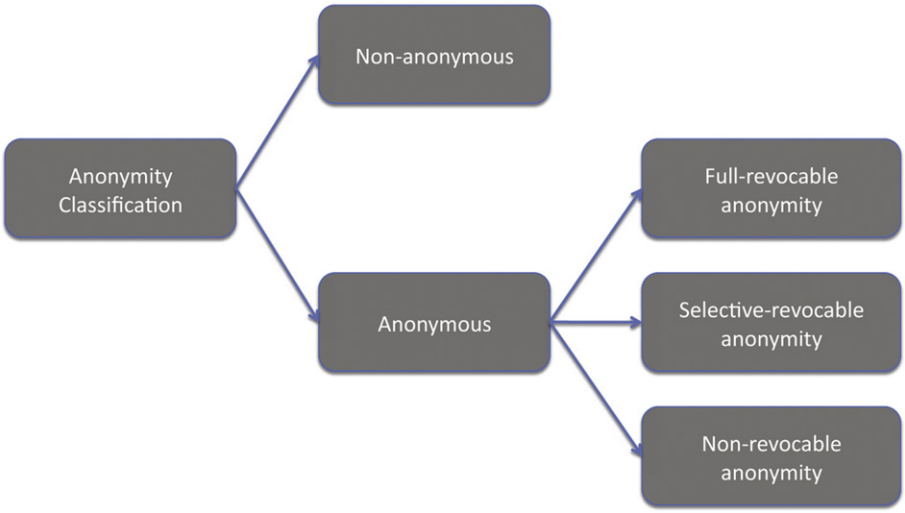

Fig. 1 – Classification of the proposals by anonymity.

describe the ET proposals that the anonymity of a fraudulent user can be revoked if needed (by overspending or law enforcement). Finally, non-anonymous schemes are detailed in Section 4.4.

Table 2 summarises the classification of the protocols that we have examined. The properties of the studied schemes are also included in it. Thus, Table 2 provides a comprehensive view of this section.

4.1. *Anonymous schemes (AN)*

The schemes of this section provide anonymity to users of e-tickets. A straightforward way to achieve this property is not to include the user's identity in the e-ticket. However, most of the proposals use cryptographic techniques based on hiding the user's identity in the e-ticket. The technique that is mainly used is the blind signature based on Chaum's scheme described in Chaum (1983). Blind signature is a method of concealing a data item from the person or entity who is signing that. So, the signer signs the data regardless of what the content is.

Fan and Lei (1998) 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.

Song and Korba (2003) 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. (2004) 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 included, and anonymity then only depends on the payment method used.

Bao (2004) states that either the user or the e-ticket should be identified in order to prevent problems such as malicious attacks. So, depending on the application, the classification of the scheme presented in this paper could change. So, for some applications (e.g., cinema), the e-ticket could not include the identity of the user and the scheme is anonymous. However, in other cases, the information of the ticket holder could be inside the electronic ticket. Thus, in this case, the properties of the scheme will change and the protocol is non-anonymous. There is a real relationship between anonymity and transferability in this scheme because they don't need the user identification in the e-ticket. Reusability concerns to other ticket information, such as the user's destination. Online mode is used in this scheme for security reasons: the authors state that offline systems show weaknesses to malicious attacks.

In the proposal of Patel and Crowcroft (1997), the security requirements are defined, where anonymity is achieved, as well as offline mode, although central authority intervention is needed in order to prevent overspending.

The previous schemes will be the preferred when total anonymity is considered an essential requirement.

4.2. *Full-revocable anonymous schemes (F-RAN)*

Here, we expose solutions that provide revocable anonymity, that is, the schemes can be considered to provide weak anonymity. If all parties behave correctly, the anonymity of users will be guaranteed, but if some party misbehaves, users can lose anonymity.

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

Table 2 – Comparison of e-tickets' security requirements (see codes in Section 3).

Properties	ATH	NRP	IT	AN	NAN	S-RAN	F-RAN	TF	NTF	NOV	REU	ON	OFF	EXD	ST	EXC
(Haneberg et al., 2004)	✓	✓	✓	✓					✓	✓		✓	✓			
(Kreft, 2005)	✓	✓	✓	✓					✓	✓		✓				
(Patel and Crowcroft, 1997)	✓		✓	✓					✓	✓		✓				
(Bao, 2004)	✓	✓	✓	✓	✓			✓		✓	✓	✓				
(Siu and Guo, 2001b)	✓	✓	✓		✓		✓	✓		✓		✓	✓			
(Siu and Guo, 2001a)	✓	✓	✓		✓			✓		✓	✓	✓				
(Wang et al., 2004a)	✓		✓		✓				✓	✓		✓				
(Elliot, 1999)	✓	✓	✓		✓			✓		✓		✓				
(Pedone, 2000)	✓		✓		✓				✓	✓	✓	✓				
(Mana et al., 2001)	✓	✓	✓		✓			✓		✓	✓		✓			
(Mihlberg, 2002)	✓				✓				✓	✓		✓				
(Kuramitsu and Sakamura, 2002)	✓		✓		✓			✓		✓	✓	✓				
(Chang et al., 2006)	✓	✓	✓		✓			✓				✓		✓	✓	
(Wang et al., 2004b)	✓				✓				✓	✓		✓				
(Amoli et al., 2010)	✓	✓	✓			✓			✓			✓		✓		
(Quercia and Hailes, 2005)	✓	✓	✓			✓		✓		✓			✓			
(Fujimura and Nakajima, 1998)	✓	✓	✓				✓	✓			✓	✓			✓	
(Nakanishi et al., 1999)	✓	✓	✓				✓		✓	✓			✓			
(Jorns et al., 2007)							✓	✓		✓		✓	✓	✓		
(Heydt-Benjamin et al., 2006)	✓						✓	✓			✓	✓	✓			
(Chen et al., 2007)	✓	✓	✓				✓		✓	✓			✓			
(Vives-Guasch et al., 2010)	✓	✓	✓				✓		✓	✓			✓	✓		✓
(Vives-Guasch et al., 2012)	✓	✓	✓				✓		✓	✓	✓		✓	✓		✓

that reason, only revocable anonymity for the user could be achieved. In this case, user linkability could be easily performed if the user does not change its pseudonym regularly, because the same pseudonym would be used for different tickets. Certain volume of data could allow some of the involved participants to make user profiles if there are no pseudonym controls. For this reason, some authors use the term pseudonymity instead of anonymity.

Another technique that allows the systems to achieve full-revocable anonymity is group signatures. In a group signature based scheme a user can be authorized as a member of a group (Vives-Guasch et al., 2012) to access to a specific service, while the identity of the user remains anonymous. In this kind of anonymity revocation, the revocation is possible because a group manager can be designed to do this job. But the technique used for the revocation would allow the identification of all the members of the group, even if they behave correctly. For these reasons this technique is classified as full-revocable anonymity techniques.

Other means to achieve full-revocable anonymity are the use of anonymous credentials (Hoepman et al., 2010). This time, a set of specific attributes can be assigned to a specific user. When the user shows her anonymous credentials (attribute-based credentials) she can be authorized (the attributes provide all the system needs to know) while her identity is hidden among all the users that have the same attribute. The attribute is non-identifying but the use of the digital signature can be used to trace individuals. Like in the use of group signatures, in this kind of anonymity revocation is possible, but if it is implemented, the technique used for the revocation would allow the identification of all the members of the group. Attribute-based anonymity is one of the full-revocable anonymity techniques. In the next section anonymity techniques that allow the anonymity revocation of specific users (only those that have misbehaved) will be presented.

Depending on the services, anonymity, transferability or reusability would be required in the Fujimura et al. proposal (Fujimura and Nakajima, 1998). Pseudonyms are proposed if anonymity is required, and overspending is controlled by a central database (online mode).

Heydt-Benjamin et al. (2006) made a proposal using the 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. (2007) 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 their paper: request, issue and verification. Anonymity is achieved by the use of pseudonyms.

The system defined in Jorns et al. (2007) 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.

Kuntze and Schmidt (2007) apply trusted computing to service access control. The proposal uses a ticket system with a pseudonym created by the Trusted Agent (TA) (i.e., the user of a ticket system and associated services operating with his trusted platform), using the identities embodied in the trusted

device, and a private Certification Authority (PCA). The system achieves anonymity thanks to the pseudonyms, but the PCA knows the identity of the TA. This can be used to perform a charging for the ticket and also the PCA is able to de-anonymise misbehaving participants. In order to protect the privacy, the authors pointed out that the pseudonym could identify a group of many TAs in the system and only the PCA could potentially resolve the individual identity of a TA.

The Vives-Guasch et al. (2010, 2012) 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 he 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, this design of e-ticketing system is 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 case, 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 some of the involved participants to make user profiles if there are no pseudonym controls.

4.3. *Selective-Revocable anonymous schemes (S-RAN)*

Selective-Revocable anonymity has the advantage of avoiding the traceability problem of the pseudonyms as we have commented in the previous section. The proposals that fall into this classification usually make use of a combination of commitment schemes and zero-knowledge proofs.

The concept of commitment schemes was first formalized by Brassard et al. in (Chaum et al., 1988) and allows us to commit to a value (it cannot be changed) while keeping it hidden, with the ability to reveal the committed value later. In the e-ticketing case, the user can conceal his/her identity inside the ticket while it is remaining secret for issuers and providers.

The e-ticketing proposals introduce zero-knowledge proofs in order to prove the user is the owner of the ticket. The concept of zero-knowledge proof was first introduced by Goldwasser et al in (Micali et al., 1989). This kind of protocols allows us to control exactly how much sensitive information is being released in a protocol. In the e-ticketing case, the user is able to prove that he/she knows the committed identity information hidden inside the ticket without revealing the identity (i.e. preserving the anonymity).

However, in a selective revocable e-ticketing scheme the provider or the issuer has to be able to disclose the hidden identity of a dishonest user. To solve this problem each proposal has to properly prepare the information inside the e-ticket. For instance, Amir Salar et al. (Amoli et al., 2010), which use blind signatures in conjunction with elliptic curves, have solved this problem by designing the e-ticket in a manner that if it is used twice, the serial number of the ticket is revealed. Since the Ticket Issuer maintains the relation between the ticket serial number and its user's identity, then the provider can reveal the identity of the user by interacting with the Ticket Issuer. Otherwise, no traceability is possible because the ticket cannot be linked to any users' identity. Thus, in all these cases (i.e., selective-revocable anonymous schemes), revoking the anonymity depends on the behaviour of the user. However, in case of a full-revocable anonymous scheme, revoking the anonymity is up to a TTP (e.g. in Vives-Guasch et al. (2012) is called Pseudonym Manager).

Serban et al. (2008) present an e-ticketing system 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.

Amoli et al. (2010) propose a Location-Based Services (LBS) protocol based on one-time tickets. The ticket lets the user prove that she has been authorized to access to an LBS. The protocol provides anonymity of location as well as the ability of revoking anonymity on the ticket overspending. The ticket disconnects the relation between the location of the mobile user and its identity. The protocol is based on blind signatures and elliptic curve cryptography. A good feature of this protocol is that there is no need for the parties to trust each other in order for the protocol to operate correctly; i.e. it is not possible to make collusion even if the service provider and the ticket issuer cooperate to disclose the identity and location of the user. However, in this protocol, the user gains the trust of the ticket issuer by going through a set of cut-and-choose operations and receives the signed ticket. This technical results in a communicational and computational overhead and could be an open door to the fraud.

Quercia and Hailes' (2005) e-ticketing system proposal is based on Chaum's e-cash blind signatures, providing selective-revocable anonymity to the user (the anonymity is revoked in case of overspending), but the communication cost could be high, and it would probably slow down the system. Apart from selective-revokable anonymity, non-repudiation, offline verification as well as portability are achieved in this proposed system.

From the point of view of privacy, the previous schemes can be even better than those explained in Section 4.1, because they provide anonymity, and this anonymity can only be broken in case of fraud by the consumer.

4.4. *Non-anonymous schemes (NAN)*

The following schemes do not provide anonymity to users, but we have to bear in mind that some services require identified e-tickets, and for this reason non-anonymous schemes are not always a drawback.

In Elliot's paper (1999), 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 (2000) applies 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. (2000), 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 either 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.

Siu and Guo (2001a) propose an 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.

Also Siu and Guo (2001b) present a system with two options: the ticket can include the identity of the user or not. Obviously, in the first case, the scheme is not anonymous. But, in the second case, each user has a wallet to store the e-tickets and the e-tickets have the identification of the wallet. Now, the Issuer of the wallet knows the relation that links the wallet and the user, so it can revoke the anonymity of the ticket.

Mana et al. (2001) 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 (2002) 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 it describes problems in contactless communication disconnections (causing inconsistency), and it also comments the need for use of standarized formats in order to solve the management of specific tickets from different applications. This proposal provides transferability, but not anonymity.

Matsuo and Ogata (2003) present an e-ticketing system that could fit with Automatic Fare Collection systems. 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 AFC 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.

The proposal by Wang et al. (2004a) presents 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.

Chang et al. (2006) present an online e-ticketing system for mobile users, considering security aspects like ticket theft, verification of the ticket owner. 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 also has information of the ticket's expiration date.

Wang et al. (2004b) presented a system that is non-anonymous, where the authentication method is made by the use of a smart-card.

Haneberg (2008) presents applications for railway tickets (transport), taking into account advantages and disadvantages in the properties that smart-cards, PDAs and mobile phones have, focussing on their tamper-proof security requirements. Overspending is controlled by a central server (online mode), and anonymity is not considered in this system.

The SIESTA (Bald et al., 2010) is a research project co-funded by Tuscany Region in Italy, providing automated services to tourists visiting. Some of the provided services using mobile phones (equipped with NFC and GPS technology) are automated payments and ticketing. Concerning the electronic tickets, the developed application allows tourists to use their own phone as a ticket for museums, theatres, public transports or car parks. The protocol is divided in two phases: the Acquisition phase, when the ticket is purchased and downloaded in the internal NFC memory of the phone, and the Access phase, when the user uses the ticket. In this e-ticketing system, the identification number of the NFC device identifies the user. The user information is stored in a database along with the number of his device. So, the authentication is very simple and there is no privacy. Moreover, the method to avoid overspending is quite straightforward: the NFC reader of the system provider deletes the ticket from the user's device.

In these systems, anonymity could not be achieved due to different reasons. Some proposals were oriented to services where anonymity could not be provided to the user, or simply, these systems were 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.

5. Summary

The use of electronic tickets allows the users to buy, receive and validate the ticket without need to move to a certain place to make these phases, neither to print it. The paper costs reduction in addition to the improved processes management

(payment, issue, validation, high amount of tickets management, etc) are the main advantages for users as well as service providers. But the ticket in electronic format requires users to carry a device in order to save and manage these tickets.

A state-of-the-art in electronic tickets has been performed, where the existing proposals and projects have been analysed. The study comprises the evaluation of the information included in the tickets, their security requirements, their phases or processes, their involved participants in these systems, and their possible oriented services.

Information in electronic tickets, based on the analysed proposals, includes the ticket serial number, the issuer entity, the service provider, the user (in non-anonymous systems), the offered service, this service's terms and conditions, the type of ticket (its transferability and its number of valid uses), the destination (in transport services), some optional attributes (depending on the service), its validity time, the ticket's date of issue, the issuer's digital signature, and finally a device identification (if the ticket is linked only with a selected device).

In terms of security, an electronic ticketing system has to comply with the requirements defined previously, that is, authenticity, non-repudiation, integrity, anonymity (considering the options: anonymous, non-anonymous, full-revocable anonymous and selective-revocable anonymous, depending on the service), transferability (if the ticket could be transferred to another user or not, depending on the service too), number of uses (if overspending is allowed or not, also depending on the service), online/offline mode (the analysed proposals are more oriented to offline mode for security terms unless its loss in validation efficiency), and the ticket state. A table has been included in order to show the comparison between the security requirements of the analysed proposals. These proposals have been described and classified depending on the anonymity requirement.

There is no unanimity in terms of the number of phases of the analysed proposals, due to the multiple services that could be offered, but there are some phases that can be considered as basic: ticket payment, issue/reception, and validation. Some proposals join payment and issue/reception, or alternatively a previous registration phase is added at the moment of the ticket reception.

The participants involved in an e-ticketing system are: the user (who obtains and validates the ticket), the ticket issuer, and the service provider (who validates the user's ticket and provides the service). Some proposals also consider the existence of intermediaries, certification authorities, etc.

Although some e-ticketing systems are being used for different services, they have some common security requirements: authenticity, non-repudiation, integrity and state. Other requirements depend on the service.

Anonymity and transferability properties are linked, that is, in order to transfer an e-ticket, this one has to be non-identified. The ticket will not be transferable if it is linked to a certain person. Anonymity cannot be achieved in cases of air travel or shipping companies. In all of these cases, users have to be identified and authenticated before using the service. In rail, bus, subway and taxi companies, the ticket could be anonymous except for multitravel tickets linked to a certain person.

The number of uses is another property that could be configured, specially for mediaries, transport and leisure companies. These companies offer different services that require different modes of use. For example, a single ticket could be used only once, but multitravel tickets are used many times. Another example could be the seasonal tickets, depending on the ticket validity time.

Online/offline verification depends on the availability of a communications network in the place where this verification is being held. Online verification is recommendable if there is an available connection to the server. For mediaries or transport companies, this property should be configured, not treated as default, because there will be places with available connection (air travel, shipping, rail and subway), places where it is being implemented (bus) and other places without it (taxi).

The great majority of systems are oriented to transport services, especially rail transport, and followed by air travel, bus and subway. Some of the tolls payment systems proposals use the name of electronic tickets, but they are closer to a payment system than a ticketing system. Finally, an important note would be the incremental use of electronic tickets in the leisure sector that has being carried out, specially on sports or cultural events.

With the actual deployment of devices such as smart phones or NFC readers, e-ticketing is one of the technologies with the best expectatives of use in the near future.

Acknowledgements

This work was partially supported by the Spanish Ministry of Science and Innovation [TSI2007-65406-C03- 01, ARES-CONSOLIDER INGENIO 2010 CSD2007-00004, RIPUP TIN2009-11689, Audit Transparency Voting Process IPT-430000-2010-31]; the Spanish Ministry of Industry, Commerce and Tourism [eVerication2 TSI-020100-2011-39, SeCloud TSI-020302-2010-153]; and the Government of Catalonia [2009 SGR1135]. The authors are solely responsible for the views expressed in this paper, which do not necessarily reflect the position of UNESCO nor commit that organization.

REFERENCES

AirCanada. Mobile check-in, http://www.aircanada.com/en/travelinfo/traveller/mobile/mci.html; 2007.

Amoli AS, Kharrazi M, and Jalili R. 2ploc: preserving privacy in location-based services. In IEEE 2nd International Conference on Social Computing/PASSAT'2010; 2010. p. 707–712.

AMSBUS, 2008. http://www.svt.cz/en/amsbus/.

Arnab A and Hutchison A. Ticket based identity system for drm. In: Proceedings Information Security South Africa. Sandton, South Africa; 2006.

Bald D, Benelli G, and Pozzebon A. The siesta project: near field communication based applications for tourism. In: IEEE 7th International Symposium on Communication Systems Networks and Digital Signal Processing (CSNDSP); 2010. p. 721–725.

Bao F. A scheme of digital ticket for personal trusted device. In: 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC04), vol. 4. IEEE; 2004. p. 3065–9.

Caron J, Lagrange I, Robet L. Contactless cell phone payment and e-ticketing: Japan leads the way at cartes & identification; 2007. 2007. CARTES 2007 Press release.

Chang CC, Wu CC, Lin IC. A secure e-coupon system for mobile users. International Journal of Computer Science and Network Security 2006;6(1):273–80. IEEE.
Chaum D, Brassard G, Crépeau C. Minimum disclosure proofs of knowledge. Journal of Computer and System Sciences 1988;37: 156189.
Chaum D. Blind signatures for untraceable payments. Advances in Cryptology - CRYPTO'82 1983:199–203.
Chen YY, Chen CL, Jan JK. A mobile ticket system based on personal trusted device. Wireless Personal Communications: An International Journal 2007;40(4):569–78.
Elliot J. The one-card trick multi-application smart card e-commerce prototypes. Computing & Control Engineering Journal 1999;10(3):121–8. IET.
Fan CI, Lei CL. Micro-recastable ticket schemes for electronic voting. IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences 1998;E81A(5):940–9.
Ferrer-Gomilla JL, Onieva JA, Payeras-Capellˆ MM, López-Mu nóz J. Certified electronic mail: properties revisited. Computers & Security 2010:167–79.
Fujimura K, Nakajima Y. General-purpose digital ticket framework. In: 3rd USENIX Workshop on Electronic Commerce. USENIX; 1998. p. 177–86.
Fujimura K, Kuno H, Terada M, Matsuyama K, Mizuno Y, Sekine J. Digital-ticket-controlled digital ticket circulation. In: 8th USENIX Security Symposium. USENIX; 1999. p. 229–40.
Fujimura K, Nakajima Y, Sekine J. Xml ticket: generalized digital ticket definition language. W3C XML-Dsig'99; 1999.
FynBus. Sms-billet, 2007. http://www.fynbus.dk/.
Granados N, Gupta K, Kauffman R. It-enabled transparent electronic markets: the case of the air travel industry. Inf. Syst. E-Business Management 2007:65–91.
Haneberg D, Stenzel K, Reif W. Electronic-onboard-ticketing: software challenges of an state-of-the-art m-commerce application. In: Pousttchi K, Turowski K, editors. Workshop mobile commerce, volume 42 of Lecture notes in Informatics (LNI). Gesellschaft für Informatik (GI); 2004. p. 103–13.
Haneberg D. 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.
Haneberg D. Electronic ticketing: risks in e-commerce applications. Digital excellence. pages 55–66. Springer-Verlag; 2008.
Heydt-Benjamin TS, Chae HJ, Defend B, Fu K. Privacy for public transportation. In: 6th Workshop on privacy enhancing technologies (PET 2006). LNCS 4258; 2006. p. 1–19.
Hoepman J-H, Jacobs B, and Vullers P. Privacy and security issues in e-ticketing – Optimisation of smart card-based attribute-proving. In: Workshop on Foundations of Security and Privacy, FCS-PrivMod 2010. Edinburgh, UK, July 14-15, 2010. Proceedings, 2010.
IATA. E-ticketing, http://www.iata.org/stbsupportportal/e-ticketing.htm; 2007.
IATA. Industry bids farewell to paper ticket, http://www.iata.org/pressroom/pr/2008-31-05-01.htm; 2008.
Jorns O, Jung O, and Quirchmayr G. A privacy enhancing service architecture for ticket-based mobile applications. In: 2nd International Conference on Availability, Reliability and Security. Vienna, Austria, vol. 24; Apr 2007. p. 374–383. ARES 2007-The International Dependability Conference.
Kreft H. Cashing up with mobile money - the faircash way. Euro mGov 2005, page 29. Brighton (UK): Sussex University; 2005 [Mobile Government Consortium International LLC].
Kuntze N, Schmidt AU. Trusted ticket systems and applications. New Approaches for Security, Privacy and Trust in Complex Systems 2007;232. IFIP International Federation for Information Processing.
Kuramitsu K, Sakamura K. Electronic tickets on contactless smartcard database. In: Proceedings of the 13th International Conference on Database and Expert Systems Applications. LNCS 2453; 2002. p. 392–402.
Kuramitsu K, Murakami T, Matsuda H, and Sakamura . Ttp: secure acid transfer protocol for electronic ticket between personal tamper-proof devices. In: 24th Annual International Computer Software and Applications Conference (COMPSAC2000). Taipei, Taiwan, vol. 24; Oct 2000. p. 87–92.
LeedsUnited. Official leeds sms, http://www.leedsunited.com/page/Welcome; 2007.
Lutgen J. 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. Vienna, Austria: Vieweg&Teubner Verlag; 2007. p. 411–9.
Mana A, Martínez J, Matamoros S, Troya JM. Gsm-ticket: generic secure mobile ticketing service. In: Gemplus World Developers Conference. Paris (France): Gemplus; 2001.
Matsuo S, Ogata W. Electronic ticket scheme for its. IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences 2003;E86A(1): 142–50.
McDaniel RL and Haendler F. Advanced rf cards for fare collection. In: Commercial Applications and Dual-Use Technology, Conference Proceedings, Telesystems Conference; 1993. p. 31–35.
Micali S, Goldwasser S, Rackoff C. The knowledge complexity of interactive proof systems. SIAM J.Computing 1989;18:186–208.
Mihlberg F. On the formal analysis of e-ticketing protocols. Master's thesis, School of Computer Science and Engineering; 2002.
Nakanishi T, Haruna N, Sugiyama Y. Unlinkable electronic coupon protocol with anonymity control. In: Proceedings of the Second International Workshop on Information Security. LNCS 1729; 1999. p. 37–46.
NY.Times. Paper is out, cellphones are in, http://www.nytimes.com/2008/03/18/technology/18check.html; 2008.
Patel B and Crowcroft J. Ticket based service access for the mobile user. In: Proceedings of the 3rd Annual ACM/IEEE international conference on mobile computing and networking (MOBICOM'97). Budapest, Hungary; 1997. p. 223–233.
Pedone F. A two-phase highly-available protocol for online validation of e-tickets. Hewlett-Packard Labs Technical Reports; 2000. HPL-2000-116 20000929.
Prague. Public.Transport. Sms tickets for public transport in Prague, http://www.prague.net/sms-ticket; 2007.
Quercia D and Hailes S. Motet: mobile transactions using electronic tickets. In: 1st international Conference on Security and Privacy for emerging Areas in Communications Networks, Proceedings. Athens, Greece, vol. 24; Sep 2005. p. 374–383.
Serban C, Chen Y, Zhang W, Minsky N. The concept of decentralized and secure electronic marketplace. Electronic Commerce Research 2008;8(1–2):79–101.
Siu IW, Guo ZS. The secure communication protocol for electronic ticket management system. In: 8th Asia-Pacific Software Engineering conference (APSEC2001). University of Macau; 2001.
Siu WI and Guo ZS. Application of electronic ticket to online trading with smart card technology. In: Proceedings of the 6th INFORMS Conference on Information Systems and Technology (CIST-2001). Miami Beach, Florida (US); 2001. p. 222–239.
Song R, Korba L. Pay-tv system with strong privacy and non-repudiation protection. IEEE Transactions on Consumer Electronics 2003;49(2):408–13.
Spanair. Spanair y vodafone españa presentan la tarjeta de embarque móvil, http://www.spanair.com/web/es-es/Sobre-

Spanair/Noticias-y-eventos/Spanair-y-Vodafone-Espana-presentan-la-tarjeta-de-embarque-movil/; 2007.
Valdecasas-Vilanova MEG, Endsuleit R, Calmet J, and Bericht I. State of the art in electronic ticketing. Master's Thesis, Institut für Algorithmen und Kognitive Systeme; 2003.
Vives-Guasch A, Payeras-Capellà MM, Mut-Puigserver M, Castellà-Roca J. E-ticketing scheme for mobile devices with exculpability. In: Data Privacy Management (DPM), Fifth International Workshop. LNCS 6514; 2010. p. 79–92.
Vives-Guasch A, Payeras-Capellà MM, Mut-Puigserver Macià, Castellà-Roca Jordi, Ferrer-Gomila JL. A secure e-ticketing scheme for mobile devices with near field communication (nfc) that includes exculpability and reusability. IEICE 2012;E95-D(1).
von Dörnberg A. The global phenomenon of low cost carrier growth. Trends and issues in global tourism. Springer-Verlag Berlin and Heidelberg GmbH & Co. KG; 2007. pages 53–59.
Wang G, Bao F, Zhou J, Deng RH. Proxy signatures scheme with multiple original signers for wireless e-commerce applications. In: Vehicular Technology Conference, VTC2004-Fall, vol. 5. IEEE; 2004. p. 3249–53.
Wang SC, Yan KQ, and Wei CH. Mobile target advertising for mobile user. In: International Workshop on Business and Information (BAI 2004), V2. Taipei, Taiwan; 2004.

Macià Mut Puigserver (Mallorca, 1966). He achieved his graduate in Computer Science in 1990 at the Autonomous University of Barcelona. He received his Ph.D. in 2006 at the University of Balearic Islands (UIB). In 1996 he joined to the Department of Mathematic and Computer Science at the UIB. He began teaching as a Vocational Training Professor specialized in Computer Science in 1990. His current research interests are: design of secure protocols, secure e-commerce, mobile applications and applied cryptography. He is author of articles on these topics in international journals and in international and national conferences.

M. Magdalena Payeras-Capellà (Mallorca, 1973). She got her title as Telecommunication Engineer (1998) from the Polytechnic University of Catalonia (UPC) and her Ph.D. in Computer Science (2005) from the University of the Balearic Islands (UIB). She has held several posts in the University of the Balearic Islands since 1998 in the department of mathematics and computer science. Her research is focused in the security in communications networks, protocols for e-commerce and its technical-legal. She has published in international journals and in international and national conferences, some of them published in international journals included in Journal Citation Reports.

Josep-Lluís Ferrer-Gomila was born in Palma (Spain) in 1967. He got his BSc degree as Telecommunication Engineer (1991) from the Polytechnic University of Catalonia (UPC) and PhD degree in Computer Science (1998) from the University of the Balearic Islands (UIB). He is associate professor in the University of the Balearic Islands since 1995 in the department of mathematics and computer science. His main topic of research is security in electronic commerce. He is author of publications in international journals and in international and national conferences, some of them published in international journals included in Journal Citation Reports.

Arnau Vives Guasch (Valls, Catalonia, 1983) is a PhD student at the CRISES Research Group (UNESCO Chair in Data Privacy) of the Universitat Rovira i Virgili. He achieved his title of Engineer in Computer Science from Universitat Rovira i Virgili in 2006, and his Master degree in Computer Engineering and Security in 2008 from the same University. His research motivation focuses on the fields of applied cryptography, privacy, secure e-commerce protocols and mobile applications. He has published and participated in several international and national conferences, and he is author of a patent.

Jordi Castellà Roca (Menàrguens, Catalonia, 1975) is tenured assistant professor at Rovira i Virgili University, he is member of UNESCO Chair in Data Privacy. He got his title of Engineer in Computer Systems from University of Lleida in 1998, the title of Engineer in Computer Science from Rovira i Virgili University in 2000 and Ph.D. in Computer Science from the Autonomous University of Barcelona in 2005. His research focuses on the fields of cryptography and privacy. He has published over 40 works, is co-author of six patents, and has participated in 24 research projects (main researcher in six of them).