Electronic road pricing system for low emission zones to preserve driver privacy

Roger Jardí-Cedó[1], Macià Mut-Puigserver[2], M. Magdalena Payeras-Capellà[2], Jordi Castellà-Roca[1], Alexandre Viejo[1]

[1] Dpt. d'Enginyeria Informàtica i Matemàtiques, UNESCO Chair in Data Privacy, Universitat Rovira i Virgili, Av. Països Catalans 26, E-43007 Tarragona, Spain
{roger.jardi,jordi.castella,alexandre.viejo}@urv.cat

[2] Dpt. de Ciències Matemàtiques i Informàtica, Universitat de les Illes Balears, Ctra. de Valldemossa, km 7,5. E-07122 Palma de Mallorca, Spain
{macia.mut, mpayeras}@uib.es

Abstract. At present, great cities try to prevent from high levels of pollution and traffic jam by restricting the access of vehicles to centric zones. They are also known as Low-Emission Zones (LEZ). Some of the most important issues of LEZs are the risk of losing privacy of the citizen who drives through the LEZ and a significant error percentage on detection of fraudulent drivers. In this article, an Electronic Road Pricing (ERP) system designed specifically for cities with Low-Emission Zones is proposed. The aim of this system is to detect fraud and to preserve driver privacy. In this case, revocable anonymity makes only fraudulent drivers lose their privacy.

Keywords: electronic road pricing, data privacy, security, low emission zone

1 Introduction

Cities such as Paris, Barcelona or Rome have circulation problems, with traffic jams and pollution problems due to the huge vehicle concentration in certain areas. The air quality guidelines presented by OMS in 2005, give guidance on "the way to reduce air pollution effects on health". Based on these recommendations, different European directives, such as 2008/50/CE, limit the level of certain environmental pollutants. In order to fulfill this legislation, the different administrations are implanting, among other measures, HOV lanes [3], variable speed or vehicle circulation restrictions in central areas. This last measure, known as **Low-Emission Zone (*LEZ*)** and adopted in many cities like Singapore, Tokyio or Beijing[10, 11, 5], makes vehicles pay so as to circulate according to certain conditions, such as weight or emissions.

Since some decades ago, Electronic Toll Collection (ETC) has been used in highways, tunnels or bridges in order to expedite toll payments as well as to reduce traffic jams. Likewise, thanks to new technologies such as the GPS and wireless communication, vehicular location-based services (VLBS) have been developed with the purpose of providing information to drivers in relation to their geographic location and improving transportation efficiency. Those ETC

systems, considered VLBS, are known as **Electronic Road Pricing (ERP)**. They present some improvements such as a more flexible calculus of the fees according to the distance driven, route or time. Moreover, these systems, applied in urban areas, allow managing traffic in central areas through the control of the flow and the density of vehicles, thus reducing traffic jams. This can be achieved by modifying the price of the fees dynamically (the rise on the price of those dense areas suggests drivers to avoid them). However, as it is later shown, these systems have certain privacy problems.

1.1 State of the Art

In recent years, various *ERP* systems have been proposed in the literature [9, 4, 1, 8, 6, 7]. All of them require the use of an On-Board Unit (OBU), with GPS and a system of wireless communication, with the aim of getting and sending the Service Provider, *SP* (see definition in Section 2), information related to the vehicle location and fees to pay. Pricing varies depending on the vehicle path. In [9] and [4], *OBU* sends information of the path followed to an external server, property of *SP*, which prices according to its path in every billing period. In [1, 8, 6, 7], fees are calculated locally in each *OBU* and are sent to *SP* server in every pricing period. In this case, the information disclosure related to the vehicle location is minimal. In order to achieve it, cryptographic proofs are used to demonstrate that *OBU* has been honest in the fee calculus and aggregation.

Fraud control is an important aim by *ERP* systems. Drivers, in order to save money, could act maliciously (i.e. by disconnecting or modifying *OBU* data). Consequently, mechanisms based on checkpoints, *Chp*s (see definition in Section 2), are implemented with the aim to test their honesty. *Chp*s, randomly located in the road and equipped with cameras, register the number plates of all the vehicles that cross them. These pictures are evidences that place a vehicle at a given moment and place, and are used to verify that a vehicle path has not been altered. In order to achieve this, *SP* and driver interact in the billing period. Fraud detection has a certain probability and depends on the number of *Chp*s. Further, the fact of drivers ignoring the number and its location is a basic issue.

The privacy level of drivers and detection of fraud are a compromise. When a high detection level is requested, privacy is affected, that is, *SP* be capable of rebuilding a vehicle path more precisely as long as the number of *Chp*s is greater. Besides, if *Chp*s are randomly moved every so often, and vehicle paths follow a routine (i.e. going to work), precision could be even greater though privacy would be affected.

1.2 Contributions and structure of the document

This paper proposes an *ERP* system for *LEZ*s with the aim of improving fraud control and honest drivers' privacy through revocable anonymity. Unlike other systems, *Chp*s, equipped with cameras, only register fraudulent vehicles, thus keeping honest drivers' privacy. Moreover, the *OBU* of the vehicle does not register its location, plus reconciliation between driver and system in the billing period is not required, and fraud control is non-probabilistic.

The system is presented in Section 2. The protocol is introduced in Section 3. Security is evaluated in Section 4 and conclusions are presented in Section 5.

2 System model

The proposal considers the following actors.

- *Driver D:* The person who drives a vehicle in a *LEZ*.
- *Vehicle V:* The means of transport registered by a unique D (the owner of it) but it may be driven by several Ds. V has an identifier (the vehicle plate) that connects it to the owner.
- *Secure element SE*: A tamper-proof security module installed in each V by the traffic competent authority. It performs all sensitive operations to ensure the security requirements.
- *On-board unit OBU:* This device is installed in each V. It has more computational power and storage capacity than *SE*. The device connects *SE* with the user and it performs the less sensitive protocol operations. It has a location capabilities (GPS).
- *Service Provider SP:* It offers an ERP service for urban areas thanks to a concession contract with the local public administration (i.e. City Council). This entity, apart from having the right to offer this service, is responsible for managing the system.
- *Checkpoint Chp: SP* installs in the restricted zone the checkpoints. The *Chp* aims to control the access of vehicles that enter or leave the zone.
- *Vehicle certification authority VCA:* It provides keys and certificates to Vs.
- *Punisher authority PA:* The trusted entity that knows the identity of the V owner. *PA* will reveal the identity of the V's owner in case of fraud.

2.1 Requirements

The system requirements related with fraud, privacy, authenticity and technology, are described below in order to establish the foundations of the system.

Anti-fraud Requirements When a V enters or exits a *LEZ* through a *Chp*, both obtain **proof-of-entrance** γ_i or **proof-of-leaving** γ_o. This γ_i contains information to prove that a specific V enters the *LEZ* through a specific *Chp* at a specific hour. This *proof* is considered **valid** when it cannot be modified once generated without detection (integrity), when its issuers can prove that it is their generation (authenticity), and also when they cannot deny its authoring (non-repudiation). Each proof is **linked** to a V and a *Chp*. The link between a proof and a V guarantees that the token cannot be used by another *V'*, neither in a voluntary nor in an involuntary way. This avoids the *duplicity* of a proof when a fraudulent V tries to use the same proof at the same time. *SP* assures that all the Ds pay correctly. If this is not the case, *SP* identifies the offending Ds and generates evidences to prove it. The **fraud** is done by a D when she drives in a *LEZ* without a γ_i, with an invalid γ_i, with a valid γ_i but associated with another V, or if she doesn't pay correctly in the exit. A *SP* cannot **falsely accuse** an honest D of fraud (an honest D should not be defenseless). A false accusation takes place when a *SP* unjustly claims that a V does not have a γ_i,has an invalid proof, has a valid proof belonging to another V, or if she doesn't pay correctly in the exit.

Authenticity Requirements At the entrance and at the exit of a *LEZ*, *V*s and *Chp*s exchange information. When the communication is established, both parts, *V* and *Chp* must prove its identity to the other part. This way, each one can be sure that the protocol is executed with the right entity. If this is not the case, this action must be reported.

Privacy Requirements The fraud control executed by *SP* can endanger the privacy of the *D*s. In this case, the curiosity of *SP* can cause an excessive monitoring of the system or even can trace the itinerary of a specific *V*. With the aim of avoiding this excessive control over the *V*s by *SP*, the system must (i) assure the privacy (the identity of *D* or *V* cannot be linked to any itinerary); (ii) avoid the traceability (*SP* mustn't know the itinerary of a *V*); and (iii) provide revocable anonymity to *D* (if a *D* commits fraud, *SP* needs her identity in order to punish her and for this reason, the identity is revealed).

Functional Requirements The *communication technology* used to communicate *V*s and *Chp*s needs to let *Chp* communicate with the nearest *V*. This communication is possible by combining low and medium distance communication technologies, such as Wimax, ZigBee IEEE 802.15.4 or Bluetooth IEEE 802.15.1, using directional antennae or triangulation. The *communication* and the *computation* required by the protocol must be quick enough to allow communication when the *V*s are moving. Whatever *interaction* with the *D* should be easy and agile. The *electronic payment system* required in the system should be anonymous and untraceable. Moreover, it should be quick enough to allow the transaction when the *V* exits the *LEZ*.

3 Protocol Description

Before starting the system, the system entities are initialized (3.1: Setup and 3.2: Certification). Moreover, *SP* prices the *LEZ* (3.3: Price generation), per time unit and emission category, sending each *Chp* a list of prices signed by the competent entity. *SP* repeats these operations every time prices are updated.

SE generates different credentials for *V* every time it enters a *LEZ* (3.4: Certificate generation) in order to be able to correctly authenticate with *Chp*s that manage the ins and outs of users from the *LEZ*.

When a vehicle *V* enters a *LEZ* (3.5: Check-in), it communicates with a *Chp* and they authenticate mutually. When the authentication with *V* fails, and only in this situation, *Chp* takes a picture of the *V* number plate as evidence of the infringement with which a proof-of-entrance incidence ζ_i is generated. ζ_i is sent to *PA* in order to verify the existence of fraud and so proceed with the corresponding sanction. When the authentication is correct, *V* gets an proof-of-entrance γ_i, which specifies the entry time.

When a *V* exits the *LEZ* (3.6: Check-out), it communicates with a *Chp* and they authenticate mutually. When the authentication with *V* is correct, *Chp* informs *V* about the exit time and the destination account for payment. With this information, *V* computes the amount payable for length of stay and its emission category, and makes a transaction through an electronic payment system. The

transaction reference is sent to *Chp* as a proof of payment. Finally, V receives an proof-of-leaving γ_o as a receipt. When the authentication fails, *Chp* takes a picture of V as an proof-of-leaving evidences ζ_o, which is sent to *PA*.

The payment verification is done through *SP* (3.7: Payment verification) a posteriori. For each pair of γ_i and γ_o associated to a same V, *SP* checks whether the value of the transaction coincides with the pricing, depending on the length of stay and its emission category. If the value is not correct, a proof-of-payment incidence ζ_p with these registers is created and sent to *PA*.

When *PA* receives a ζ (3.8: Sanction), it is corroborated. In case of fraud, *PA* reveals the identity of the V owner (anonymity is revoked), and evidences to refute the accusation by *SP* are requested. According to these, *PA* decides whether to sanction the owner.

3.1 Setup

The setup process works as follows:

1. *PA* obtains from competent authorities (i.e. Police):
   - An asymmetric key pair (Pk_{PA}, Sk_{PA}), its public key certificate $cert_{PA}$, and a certificate repository of the authorities
2. *SP* and *VCA* obtain from competent authorities (i.e. city council and a transit authority, respectively):
   - An asymmetric key pair (Pk_{SP}, Sk_{SP}) and (Pk_{VCA}, Sk_{VCA}), its public key certificate $cert_{SP}$ and $cert_{VCA}$, and a certificate repository of the authorities

   The certificate chain length of *VCA* is 1, and 0 in the case of *SP*. The $cert_{SP}$ validity period can correspond to the concession lifetime of the service, without exceeding it.
3. *VCA*:
   i. Defines a set of vehicles $V = \{v_1, v_2, ..., v_{n_V}\}$, where $n_V = |V|$ is the number of vehicles
   ii. Defines a collection of sets $K = \{C_1, C_2, ..., C_{n_K}\}$ partition of V, where $n_K = |K|$, with $|C_i| = n_C$, $\forall i$
   iii. Generates and associates a certification entity VCA_{C_i} to each element of the subset K $(C_1, ..., C_{n_K})$:
      iii.i. An asymmetric key pair ($Pk_{VCA_{C_i}}$, $Sk_{VCA_{C_i}}$), $\forall i \in \{1, ..., n_K\}$
      iii.ii. A CA certificate $cert_{VCA_{C_i}}$, $\forall i \in \{1, ..., n_K\}$, which has an expiration time c_{exp} and a certificate chain length of 0
4. Each *Chp* applies the following steps:
   i. Obtain a certificate repository of the authorities and entities
   ii. Generate an asymmetric key pair (Pk_{Chp}, Sk_{Chp})
   iii. Securely obtain a public key certificate $cert_{Chp}$ from *SP* containing an extension $cert_{Chp}.loc$ with its location coordinates

3.2 Certification

It is assumed that the *SE* of each V has been previously initialized with a certificate repository of the certification authorities, identifying information of the vehicle V_{id} and its technical specifications (number plate, chassis number, owner, brand, model, engine power, or level of emissions of CO_2 and other pollutant gases). The certification process of a V is done by *VCA*, before purchasing a vehicle and/or passing the regular technical tests of vehicles:

1. Register V in an element of the subset K (in a C_i)
2. Download the certification entity VCA_{C_i} associated to C_i (consisting of $Pk_{VCA_{C_i}}$, $Sk_{VCA_{C_i}}$ and $cert_{VCA_{C_i}}$), through a secure channel in the *SE*

3.3 Price generation

Whenever *SP* wants to modify the fees of a *LEZ*, it performs the next operations:

1. Set the *prices* per unit of time and emission category (i.e. European Emission Standards) and generate a timestamp ts
2. Compose *information-of-prices* $\theta = (prices, ts)$
3. Sign θ ($Sign_{SP}(\theta) = \bar{\theta}$) and send θ^*=(θ, $\bar{\theta}$) to each *Chp*

3.4 Certificate generation

This phase is performed every time a V is about to enter a *LEZ*. Thanks to the certification entity VCA_{C_i} installed in the *SE* of the V in the previous phase, this *SE* is able to perform the following operations in order to generate new public key certificates:

1. Compute an asymmetric key pair (Pk_{V_q}, Sk_{V_q})
2. Generate a public key certificate $cert_{V_q}$ with the following features:
   - An extension $cert_{V_q}.idS$ containing the probabilistic encryption (i.e. by using OAEP padding [2], standardized later in PKCS #1v2 and RFC 2437) of the vehicle identifier V_{id} with the public key of *PA*: $Enc_{Pk_{VCA}}(V_{id})$
   - An extension $cert_{V_q}.em$ containing the pollutant emission category (i.e. European Emission Standards) of the V

3.5 Check-in

When a *Chp* placed in the entrance of a *LEZ* detects a V, the protocol is applied:

1. Chp has to:
   i. Generate a nonce N_A and compose *information-of-entrance* $\psi = (N_A, \theta^*)$
   ii. Sign ψ: $Sign_{Chp}(\psi) = \bar{\psi}$, and send ψ, $\bar{\psi}$ and its $cert_{Chp}$ to V
2. *SE* of the V, with the help of the *OBU*, has to:
   i. Verify the certificate $cert_{Chp}$ and the signature $\bar{\psi}$: $Verif_{Chp}(N_A, \theta^*, \bar{\psi})$
   ii. Verify the signature $\bar{\theta}$: $Verif_{SP}(prices, ts, \bar{\theta})$ and the location coordinates $cert_{Chp}.loc$ of *Chp*
   iii. Generate a nonce N_B and compute the fingerprint $fing_{Chp}$ of $cert_{Chp}$ (it is computed as the hash function of the certificate and it is used as identifier)
   iv. Compose message $\omega_{V_q} = (\theta^*, N_A, N_B, fing_{Chp})$

v. Sign ω_{V_q}: $Sign_{V_q}(\omega_{V_q}) = \omega\bar{}_{V_q}$, and send N_B, $\omega\bar{}_{V_q}$ and its $cert_{V_q}$ to *Chp*

3. *Chp* has to:
   i. Generate a timestamp ts', and verify the certificate $cert_{V_q}$ and the signature $\omega\bar{}_{V_q}$: $Verif_{V_q}(\theta^*, N_A, N_B, fing_{Chp}, \omega\bar{}_{V_q})$
   ii. If one of the verifications fails, *Chp* performs the following operations:
      ii.i Generate an incidence number of entrance in_i
      ii.ii Take a photograph ph of V and extract the plate number plt
      ii.iii Compose *proof-of-entrance incidence* ζ_i= (in_o, plt, ph, ts', θ^*, N_A, N_B, $fing_{Chp}$, $\omega\bar{}_{V_q}$, $cert_{V_q}$)
      ii.iv Sign ζ_i: $Sign_{Chp}(\zeta_i) = \bar{\zeta_i}$, and send ${\zeta_i}^*$=(ζ_i, $\bar{\zeta_i}$) to *SP*
   iii. If the verifications performed in 3i) are correct, *Chp* has to:
      iii.i Compute the $fing_{V_q}$ of $cert_{V_q}$ and compose *proof-of-entrance* γ_i=(θ^*, N_A, N_B, $fing_{Chp}$, $\omega\bar{}_{V_q}$, $fing_{V_q}$, ts')
      iii.ii Sign γ_i: $Sign_{Chp}(\gamma_i) = \bar{\gamma_i}$ and send ts' and $\bar{\gamma_i}$ to the V

4. If the verifications performed in 3i) are correct, *SE* of the V, with the help of the *OBU*, has to:
   i. Verify the signature $\bar{\gamma_i}$: $Verif_{Chp}(\theta^*, N_A, N_B, fing_{Chp}, \omega\bar{}_{V_q}, fing_{V_q}, ts', \bar{\gamma_i})$
   ii. Verify the freshness of ts':$|ts'$-*current time*$| < \delta$, where δ is a fixed time
   iii. Store $\gamma_i^* = (\gamma_i, \bar{\gamma_i})$

3.6 Check-out

When a *Chp* placed in the exit of a *LEZ* detects a V, the next protocol is applied:

1. *Chp* has to:
   i. Generate a timestamp ts'' and a nonce N_C, and compose *information-of-payment* $\rho = (ts'', N_C, acc)$, where *acc* identifies the target account, of the electronic payment system assumed, of *SP*
   ii. Sign ρ: $Sign_{Chp}(\rho) = \bar{\rho}$, and send ρ, $\bar{\rho}$ and its $cert_{Chp}$ to V

2. *SE* of the V, with the help of the *OBU*, has to:
   i. Verify the certificate $cert_{Chp}$, the signature $\bar{\rho}$: $Verif_{Chp}(ts'', N_C, acc, \bar{\rho})$, the location coordinates $cert_{Chp}.loc$ of *Chp* and the freshness of ts'':$|ts''-$*current time*$| < \delta$, where δ is a fixed time
   ii. Recover ts' of the last γ_i and compute the length of stay τ a *LEZ*: (ts''-ts')=τ
   iii. Recover the *prices* included in θ^* of γ_i, and compute the *amount* of money required to pay according to τ, its pollutant emissions and the *prices*
   iv. Make a digital transfer of the *amount* of money to the target account *acc* and obtain a transfer reference *trans*
   v. Generate a nonce N_D and compute the fingerprint $fing_{Chp}$ of $cert_{Chp}$
   vi. Compose message $\omega_{V_q} = (ts'', N_C, N_D, fing_{Chp}$,*trans*)
   vii. Sign ω_{V_q}: $Sign_{V_q}(\omega_{V_q}) = \omega\bar{}_{V_q}$, and send N_D, *trans*, $\omega\bar{}_{V_q}$ and its $cert_{V_q}$ to *Chp*

3. *Chp* has to:
   i. Verify the certificate $cert_{V_q}$ and the signature $\omega\bar{}_{V_q}$: $Verif_{V_q}(ts'', N_C, N_D, fing_{Chp}, trans, \omega\bar{}_{V_q})$
   ii. If one of the verifications fails, *Chp* performs the following operations:

ii.i Generate an incidence number of leaving in_o
ii.ii Take a photograph ph of the V and extract the number plate plt
ii.iii Compose *proof-of-leaving incidence* ζ_o=(in_o, plt, ph, ts'', N_C, N_D, $fing_{Chp}$, $trans$, $\omega\bar{}_{V_q}$, $cert_{V_q}$)
ii.iv Sign ζ_o: $Sign_{Chp}(\zeta_o) = \bar{\zeta_o}$, and send $\zeta_o{}^*$=($\zeta_o, \bar{\zeta_o}$) to *SP*

iii. If the verifications performed in 3i) are correct *Chp* has to:
iii.i Compute the $fing_{V_q}$ of $cert_{V_q}$, and compose *proof-of-leaving* γ_o = (ts'', N_C, N_D, $fing_{Chp}$, $trans$, $\omega\bar{}_{V_q}$, $fing_{V_q}$)
iii.ii Sign γ_o, $Sign_{Chp}(\gamma_o)$=$\bar{\gamma_o}$, and send it to the V

4. If the verifications performed in 3i) are correct, *SE* of the V, with the help of the *OBU*, has to:
   i. Verify the signature $\bar{\gamma_o}$: $Verif_{Chp}(ts''$, N_C, N_D, $fing_{Chp}$, $trans$, $\omega\bar{}_{V_q}$, $fing_{V_q}$, $\bar{\gamma_o})$, and store $\gamma_o^* = (\gamma_o, \bar{\gamma_o})$

3.7 Payment verification

Each *Chp* sends *SP* the different proofs γ_i, γ_o and ζs (ζ_i and ζ_o), generated in the phases 3.5 and 3.6 of the protocol, periodically. *SP* then forwards the incidences ζ_i and ζ_o to *PA*. Moreover, *SP* performs the next operations every so often (in batch) for each set of proofs γ_i and γ_o associated with the same $fing_{V_q}$:

1. Extract ts', ts'', and $cert_{V_q}.em$ from γ_i and γ_o
2. Extract *prices* from θ^*, included in γ_i
3. Extract the reference *trans* from γ_o
4. Compute the length of stay τ a LEZ: (ts''-ts')=τ
5. Compute the $amount'$ of money required to pay according to τ, $cert_{V_q}.em$ and the *prices*
6. Verify whether the transfer *trans* was successful and recover the *amount* of money paid
7. Verify whether $amount = amount'$
8. Verify that *trans* has not been repeated in another γ_o. (i.e. with the help of a time filter according to the γ_o's *ts* and finding duplicates)
9. If one of the verifications fails then,
   i. Generate an incidence number of verification in_v
   ii. Compose *proof-of-verification incidence* ζ_p including γ_i and γ_o of V_q: ζ_p=(in_v, γ_i, γ_o). In the case of a reused *trans*, add γ'_o which proves the double spending ζ_p = (in_v, γ_i, γ_o, γ'_o)
   iii. Sign ζ_p ($Sign_{SP}(\zeta_p) = \bar{\zeta_p}$) and send $\zeta_p{}^*$=(ζ_p, $\bar{\zeta_p}$) to *PA*

3.8 Sanction

PA performs the following operations according to the origin of the received ζs:

1. In the case of ζ_i or ζ_o:
   i. Verify the signatures and extract the number plate *plt* from the photograph *ph*, included in ζ
2. In the case of ζ_p:
   i. Verify all the signatures included in ζ_p and verify that the signatory of γ_i and γ_o is the same

ii. Verify the right payment by repeating the steps 1-7 from 3.7
iii. In case of a double spending incidence, verify that the *trans* of γ_o and γ'_o are equals
iv. If the incidence is confirmed, recover the identifier V_{id} of V_q by opening the extension $certV_q.idS$ of the certificate $certV_q$, included in the proof γ_i or γ_o (in case of double spending, this is done for the last V to leave the LEZ): $Dec_{PA}(certV_q.idS) = V_{id}$

3. Contact the owner of the V from *plt* or V_{id}, inform her about the sanctioning procedure and require her evidence to the contrary to refute the accusation
4. If the owner of the V presents evidence to the contrary, these are verified. If this evidence is not valid, it fines the owner according to the type of infraction

4 Security and Requirements Analysis

The security and system requirements of the protocol are studied in this section, i.e. the entrance proofs are valid, the system preserves users' privacy, and dishonest users are identified. The discussion is organised in three propositions, and each proposition can have several claims to support its fulfilment.

Proposition 1. *The proposed system preserves authenticity, non-repudiation and integrity for the entrance and exit proofs.*

Claim. 1 The creation of fraudulent entrance and exit proofs is computationally unfeasible nowadays.

Entrance proofs have the following form $\gamma_i = (\theta^*, N_A, N_B, fing_{Chp}, \omega_{\bar{V}_q}, fing_{V_q}, ts')$. The checkpoint signs the entrance proofs γ_i: $Sign_{Chp}(\gamma_i) = \bar{\gamma}_i$ and sends the pair ts' and $\bar{\gamma}_i$ to the vehicle. In the same way, the exit proof $\gamma_o = (ts'', N_C, N_D, fing_{Chp}, trans, \omega_{\bar{V}_q}, fing_{V_q})$ is signed by the checkpoint, $Sign_{Chp}(\gamma_o)=\bar{\gamma_o}$, and sent to the vehicle. For these reasons, the generation of entrance and exit proofs is nowadays computationally unfeasible, without the knowledge of the secret key used by *Chp* in the signature.

Claim. 2 The *Chp*s, issuers of the entrance and exit proofs, can not deny the emission of these proofs.

Entrance proofs are generated and signed by their issuer (the *Chp*s) and, considering the signature scheme secure, this operation can be only performed by these issuers. Thus, the issuer's identity is linked to the proofs and, for the properties of the electronic signature scheme, it can not deny its authorship.

Claim. 3 The content of the entrance and exit proofs can not be modified by the vehicles.

If we suppose that the signature scheme is secure and that the hash summary function is collision-resistant, if the content of the entrance or exit proofs was modified, the verification of the signature would be incorrect because $Sign_e(m) = E_{Sk_e}(h(m)) = \bar{m}$. In order to pass the verification, the signature would be regenerated from the new entrance or exit ticket. This operation is computationally unfeasible without the knowledge of the checkpoint secret key.

Result 1 *According to the presented proofs in Claims 1, 2 and 3, it can be assured that the protocol satisfies the needed security requirements (authenticity, integrity and non-repudiation) for the proofs to be considered valid.*

Proposition 2. *The toll system presented here preserves the privacy of its users and protects their anonymity, avoiding the traceability of their actions.*

Claim. 4 The system guarantees the anonymity of honest users.

The information that the user transmits to enter the system is $\omega_{V_q} = (N_A, N_B, fing_{cert_{Chp}})$ and its signature. The *Chp* will verify the signature using the certificate $cert_{V_q}$ accompanying the user message. This certificate (generated by the *SE* of the *V* before entering the *LEZ*) identifies the vehicle, but the identification information is protected with an asymmetric encryption, using the public key of *PA*. Thus, *Chp* can verify the signature but it is not able to identify the vehicle. Then, *Chp* generates and transmits to the user $\bar{\gamma}_i$. With this evidence, the vehicle may enter the *LEZ*. The information related to the user identification inside $\bar{\gamma}_i$ is the same included in ω_{V_q}. This means that the *V* enters the *LEZ* without being identified.

When *V* leaves the *LEZ* (We assume that the payment system allows the anonymity of the user. The payment system is beyond the scope of this paper.), the user must send the following information: $\omega_{V_q} = (\ ts,\ N_C,\ N_D, fing_{cert_{Chp}}, trans)$ to the exit *Chp*. Assuming that the payment is anonymous, no one can identify the user through *trans*. Moreover, it is not possible to identify the user through the signature on ω_{V_q} by the reasons explained in the previous paragraph. Consequently, the entrance inside a *LEZ* and the exit from a *LEZ* of honest users are anonymous.

Claim. 5 The toll collection protocol does not allow to trace or to link the actions of the vehicles.

It is not possible to associate the various entries and exits from a *LEZ* of the same vehicle if we use the information generated by the execution of the protocol. This happens because the protocol described in 3.4 is executed each time the *V* approaches a *LEZ*. This means that the *SE* generates a new $cert_{V_q}$ for the vehicle in each new entrance process. This certificate is the only element that could identify the *V*. However, considering that the use of the certificate is unique for each entrance/leaving process, nobody can relate the identity of *V* of this entrance/leaving process with any other entrance/leaving process.

The information that could be repeated in other entrance/leaving process of the same *V* is the $certV_q.idS$ field. But, as it is specified in the protocol, $certV_q.idS$ is computed with a probabilistic encryption, using for example the OAEP padding system, which means that the result of each new encryption credentials is different.

Result 2 *The toll system presented here preserves the privacy in accordance with claims 4 and 5: users can use the system anonymously and each new usage can not be related to any other with respect to the identity of the vehicles.*

Proposition 3. *The toll system has anti-fraud requirements concerning the correctness and verifiability of the evidences generated in the protocol.*

Claim. 6 The system can identify dishonest users thanks to the anonymity revocation property of the protocol.

If users do not properly perform the authentication at the entrance/leaving process of the system, then they can lose the anonymity because the *Chp* takes a picture of the V capturing the number plate. This information is sent to *PA* to act as it is specified in the *Sanction* protocol. In the execution of this protocol, *PA* has the ability to identify the user through the number plate.

If users have not made the proper payment, then *SP* verifies in the *Payment Verification* Protocol that the amount paid corresponds to the tax determined for τ and emissions of V. If the verification fails, this information is sent to *PA* to issue a traffic fine for the user. *PA* verifies the incidence and identifies the user by opening the field $certV_q.idS$ of the certificate with its private key. Obtaining V_{id} allows the identification and the punishment of the dishonest user.

Claim. 7 The protocol execution generates evidences for an honest user (they are saved in the OBU) to prove or disprove the allegations of fraud.

When a user is accused of not performing the authentication correctly, a *pdi* that records the incidence is generated. The user can be accused of using an improper certificate $cert_{V_q}$ or sending an incorrect signature $\omega_{\bar{V}_q}$. In both cases, *PA* contacts her during the *Sanction* process, so she can provide evidences to rebut the charges.

An honest user can retrieve a valid $cert_{V_q}$, from her OBU, which matches her vehicle (identified by the number plate) or a signature $\omega_{\bar{V}_q}$ that was successfully computed by the *SE* with the help of the OBU during the entrance/leaving process of the *LEZ*. The system requirements state that the OBU of a vehicle has to have enough storage capacity to store evidences to rebut the allegations of possible fraud.

In case of a payment incidence, the user has to demonstrate that the payment has been made according to the data stored in $\bar{\rho}$ and $\bar{\gamma_o}$ (both items signed by the *Chp*). Therefore, an honest user will be able to retrieve this information from her OBU and send it to *PA* to refute the accusation.

Result 3 *The toll collection scheme keeps fraud under control and it can identify dishonest users. These users receive the appropriate traffic fine. The protocol also allows honest users to get evidences of their correct performance. The evidences are used to rebut any traffic fine due to some kind of malfunction of the system's actors.*

5 Conclusions and Further Works

This paper has presented an *ERP* system for urban areas, which provides a robust fraud control system with a high level of privacy. The entrance/leaving

process of the *LEZ* is controlled so that the legitimate tax is computed while the anonymity of the user is preserved. However, if a user commits fraud, she will then be identified by the picture of the number plate taken by the checkpoint in conjunction with the anonymity revocation system of the protocol.

As future work, we consider the extension of the protocol to take more than one *LEZ* into account. We also have the intention of implementing the scheme in order to assess its practical application.

Acknowledgments and disclaimer

This work was partially supported by the Spanish Government under CO-PRIVACY TIN2011-27076-C03-01, ARES-CONSOLIDER INGENIO 2010 CSD2007-00004 and BallotNext IPT-2012-0603-430000 projects and the FPI grant BES-2012-054780. The authors wish to acknowledge the help provided by Tamar Molina-Asens. Some of the authors are members of the UNESCO Chair in Data Privacy, yet the views expressed in this paper neither necessarily reflect the position of the UNESCO nor commit with that organization.

References

1. Balasch, J., Rial, A., Troncoso, C., Preneel, B., Verbauwhede, I., Geuens, C.: Pretp: Privacy-preserving electronic toll pricing. In: USENIX Security Symposium. pp. 63–78 (2010)
2. Bellare, M., Rogaway, P.: Optimal asymmetric encryption. In: EUROCRYPT. Lecture Notes in Computer Science, vol. 950, pp. 92–111. Springer (1995)
3. BOE: Resolución int/2836/2013, CVE-DOGC-B-14013017-2014. Núm 6541 - 15.1.2014
4. Chen, X., Lenzini, G., Mauw, S., Pang, J.: A group signature based electronic toll pricing system. In: ARES. pp. 85–93. IEEE Computer Society (2012)
5. Costabile, F., Allegrini, I.: A new approach to link transport emissions and air quality: An intelligent transport system based on the control of traffic air pollution. Environmental Modelling and Software 23(3), 258–267 (2008)
6. Day, J., Huang, Y., Knapp, E., Goldberg, I.: Spectre: spot-checked private ecash tolling at roadside. In: WPES. pp. 61–68. ACM (2011)
7. Garcia, F.D., Verheul, E.R., Jacobs, B.: Cell-based privacy-friendly roadpricing. Computers & Mathematics with Applications 65(5), 774–785 (2013)
8. Meiklejohn, S., Mowery, K., Checkoway, S., Shacham, H.: The phantom tollbooth: Privacy-preserving electronic toll collection in the presence of driver collusion. In: USENIX Security Symposium. pp. 32–32 (2011)
9. Popa, R.A., Balakrishnan, H., Blumberg, A.J.: Vpriv: Protecting privacy in location-based vehicular services. In: USENIX Security Symposium. pp. 335–350. USENIX Association (2009)
10. Santos, G.: Urban congestion charging: A comparison between london and singapore. Transport Reviews 25(5), 511–534 (2005)
11. Wolff, H.: Keep your clunker in the suburb: Low-emission zones and adoption of green vehicles. The Economic Journal pp. n/a–n/a (2014), http://dx.doi.org/10.1111/ecoj.12091