UNIVERSITAT ROVIRA I VIRGILI

Lightweight and Privacy-Preserving Access Protocols for Low Emission Zones

Carles Anglés Tafalla

UNIVERSITAT
ROVIRA i VIRGILI

Lightweight and Privacy-Preserving Access Protocols for Low Emission Zones

Carles Anglés Tafalla

DOCTORAL THESIS
2019

Carles Anglés Tafalla

Lightweight and Privacy-Preserving Access Protocols for Low Emission Zones

DOCTORAL THESIS

Supervised by Dr. Jordi Castellà-Roca

Co-Supervised by Dr. Alexandre Viejo

Department of Computer Engineering and Mathematics

UNIVERSITAT ROVIRA i VIRGILI

December 2019

I STATE that the present study, entitled "Lightweight and Privacy-Preserving Access Protocols for Low Emission Zones", presented by Carles Anglés Tafalla for the award of the degree of Doctor, has been carried out under my supervision at the Department of Computer Engineering and Mathematics of this university, and that it fulfills all the requirements to be eligible for the International Doctorate Award.

Tarragona, December 22, 2019

Doctoral Thesis Supervisor	Doctoral Thesis Supervisor
Dr. Jordi Castellà-Roca	Dr. Alexandre Viejo

Acknowledgements

I would particularly like to thank my advisors Dr. Jordi Castellà and Dr. Alexandre Viejo for their guidance and support during the development of this thesis.

I wish to thank Dr. Magdalena Payeras and Dr. Macià Mut from Illes Balears University for their collaboration and assistance. I also wish to show my appreciation to Josep Domingo-Ferrer and all CRISES group members, especially to Jesús Manjón, Alberto Blanco and Romina Russo for their help and advice. Finally, I am grateful to Dr. Jan Hajny, Dr. Petr Dzurenda, Dr. Sara Ricci and the rest of the Cryptology Research Group of Brno University of Technology for their hospitality and kindness during my 3 months research stay in the Czech Republic.

Last but not least, I would like to thanks my family and friends for always being there when I needed them, especially to my parents and sister for all their support and love.

This work was partially supported by the DGT under the project ISSUM

SPIP2017-02250 and the Spanish Government under AccessTur (TIN2014-54945-R AEI/FEDER UE), SmartGlacis (TIN2014-57364-C2-R), CONSENT (RTI2018-095094-B-C21) and Red de excelencia Consolider ARES TIN2015-70054-REDC projects.

Contents

List of Figures

List of Tables

Abstract

In the last years, Low Emission Zones (*LEZ*), i.e. areas where some restrictions and surcharges are applied to their users in accordance to their vehicle emissions, have emerged as one of the most popular mechanisms to tackle urban traffic congestion and its subsequent impact on the cities' environmental pollution. The rapid proliferation of LEZs through all Europe, especially in Central-Europe countries like Germany, The Netherlands, Belgium and the north of Italy, are clear examples of this increasing trend. Even other countries like Spain, which still does not implement them in their soil, is tailoring a draft bill which stipulates LEZs as mandatory for its bigger cities.

Even though LEZs have proven to be an effective measure against those issues, they have also been criticized in the literature due to the relevant privacy threat that they pose to the drivers passing by. In particular, current deployed systems used to enforce LEZs strongly depend on the indiscriminate use of camera networks to track the drivers' whereabouts, requiring infrastructures that can hinder their deployment in real scenarios. Moreover, these solutions also reveal a strong dependence on centralized entities to manage the vehicles' access acknowledgment, fare ascertaining and fee payment. The inherent reliance on those entities poses a single point of failure, jeopardizing the systems' security and stability.

The aim of this thesis is to contribute with novel privacy-preserving protocols for LEZ Access Control schemes which tackle the deployability and centralization issues found in the current literature works, while providing effective anti-fraud measures to preserve the privacy of the drivers who behave honestly. Under these premises, in the first contribution, we propose an access control system for LEZs lightweight enough to be used in low-cost infrastructures while the only equipment required by users is a common smartphone. One of the cornerstones of this approach is its deployability in real scenarios, for this reason, the feasibility of the new technology is validated in a relevant environment and an extensive evaluation is provided. In what regards our second and third contributions, two access control protocols for LEZs are proposed in order to shed the centralized position that third parties, responsible of registering vehicle accesses and charging fees, hold in favor of the blockchain decentralized paradigm. The privacy-preserving mechanisms used in those works address the user's privacy requirements that a public ledger like blockchain demands.

Resum

Les Zones de Baixes Emissions (ZBE), és a dir, àrees on s'apliquen certes restriccions o recàrrecs als seus usuaris d'acord amb les emissions dels seus vehicles, s'han convertit en un dels mecanismes més populars per abordar la congestió viària i el seu conseqüent impacte en la contaminació mediambiental a les grans ciutats. La ràpida proliferació de ZBE a Europa, especialment en països d'Europa central com Alemanya, els Països Baixos, Bèlgica i el nord d'Itàlia, són clars exemples d'aquesta tendència. Fins i tot altres països com Espanya, que encara no les implementa al seu territori, està confeccionant un projecte de llei que estipula que les ZBE seran obligatòries per a totes les seves grans ciutats.

Tot i que les ZBE han demostrat ser una mesura efectiva contra aquesta problemàtica, també han estat motiu de crítica en la literatura actual ja que representen una amenaça per a la privacitat dels seus usuaris. Més concretament, els sistemes de control actualment desplegats per fer complir les restriccions imposades per les ZBEs depenen en gran mesura de l'ús indiscriminat de xarxes de càmeres per verificar la ubicació real dels usuaris, requerint d'un gran nombre d'infraestructures que pot dificultar-ne el desplegament en escenaris reals. A més a més, s'uneix la problemàtica que tots aquests sistemes presenten una forta dependència cap a entitats centralitzades per a la verificació d'accés de vehicles, el càlcul de tarifes

i el pagament d'aquestes. La dependència cap a aquestes entitats suposa la introducció d'un "Single Point of Failure" que representa una amenaça per a la seguretat i l'estabilitat d'aquests tipus de sistemes de control.

L'objectiu d'aquesta tesi és contribuir amb nous protocols per gestionar el control d'accés a ZBE que abordin els problemes d'implementació i centralització presents en els treballs de la literatura actual, proporcionant, alhora, mesures efectives contra el frau que preservin la privacitat dels usuaris que actuïn honestament. Sota aquestes premisses, en la nostra primera contribució proposem un sistema de control d'accés per ZBE suficientment lleuger computacionalment com per ser utilitzat en infraestructures de baix cost i en Smartphones comuns en la part dels usuaris. Donat que una de les pedres angulars d'aquesta proposta radica en la seva capacitat de desplegament en escenaris reals, també es contribueix amb una avaluació exhaustiva sobre la viabilitat del sistema proposat en un entorn de proves rellevant. Pel que fa a la nostra segona i tercera contribució, es proposen dos protocols de control d'accés per ZBE amb l'objectiu de posar fi a la centralització que ostenten algunes terceres parts en els processos de registre d'accés de vehicles i còmput de tarifes en favor del paradigma descentralitzat que confereix el Blockchain. Els mecanismes per a la preservació de la privacitat utilitzats en aquestes propostes garanteixen els requisits de privacitat per als usuaris que un registre comptable públic com el Blockchain requereix.

Resumen

Las Zonas de Bajas Emisiones (ZBE), es decir, áreas donde se aplican ciertas restricciones o recargos a sus usuarios de acuerdo con las emisiones de sus vehículos, se han convertido en uno de los mecanismos más populares para abordar la congestión vial y su consecuente impacto en la contaminación medioambiental en las grandes ciudades. La rápida proliferación de ZBE en Europa, especialmente en países de Europa central como Alemania, los Países Bajos, Bélgica y el norte de Italia, son claros ejemplos de esta tendencia. Incluso otros países como España, que todavía no las implementa en su territorio, está confeccionando un proyecto de ley que estipula que las ZBE serán obligatorias para todas sus grandes ciudades.

Aunque las ZBE han demostrado ser una medida efectiva contra esta problemática, también han sido motivo de crítica en la literatura actual debido a que representan una amenaza para la privacidad de sus usuarios. Más concretamente, los sistemas de control desplegados actualmente para hacer cumplir las restricciones que implementan las ZBEs dependen en gran medida del uso indiscriminado de redes de cámaras para verificar la ubicación real de los usuarios, requiriendo un gran número de infraestructuras que puede dificultar su despliegue en escenarios reales. Además de esta problemática, se une que todos estos sistemas revelan una fuerte dependencia hacia entidades centralizadas para la verificación de acceso de

vehículos, el cálculo de tarifas y el pago de las mismas. Dicha dependencia hacia estas entidades supone la introducción de un "Single Point of Failure" que representa una amenaza para la seguridad y la estabilidad de los sistemas de control de ZBEs.

El objetivo de esta tesis es contribuir con nuevos protocolos para el control de acceso en ZBE con el fin de abordar los problemas de implementación y centralización presentes en los trabajos de la literatura actual, proporcionando, a la vez, medidas efectivas contra el fraude que preserven la privacidad de los usuarios que actúen honestamente. Bajo estas premisas, en nuestra primera contribución proponemos un sistema de control de acceso para ZBE lo suficientemente ligero computacionalmente como para ser utilizado en infraestructuras de bajo coste y en Smartphones comunes en el lado de los usuarios. Debido a que una de las piedras angulares de esta propuesta radica en su capacidad de despliegue en escenarios reales, también se contribuye con una evaluación exhaustiva sobre la viabilidad del sistema propuesto en un entorno relevante. En lo que respecta a nuestra segunda y tercera contribución, se proponen dos protocolos de control de acceso para ZBE con el objetivo de poner fin a la centralización que ostentan algunas terceras partes en los procesos de registro del acceso de vehículos y cómputo de tarifas en favor del paradigma descentralizado que confiere el Blockchain. Los mecanismos para la preservación de la privacidad utilizados en dichas propuestas garantizan los requisitos de privacidad para los usuarios que un registro contable público como el Blockchain requiere.

Chapter 1

Introduction

1.1 Motivation

The registered high levels of environmental pollution, due in large part to urban traffic congestion, have become a serious problem for large metropolitan areas all over the world [1, 2]. In the center of those cities, the levels of air pollution exceed some of the World Health Organization (WHO) thresholds [3] posing a serious threat to their citizens' health [4, 5, 6]. In the light of such problematic, governmental and state administrations started adopting different measures and mechanisms to promote the rational use of vehicles and incentivize the use of less contaminating ones. The nature of those mechanisms encompass a wide variety of approaches which range from incentives for less contaminating vehicles, like electrical dedicated parking places or High-Occupancy Vehicle (HOV) lanes, to heavy restrictions for contaminating ones, e.g. even/odd license plate circulating restrictions.

In the recent years, Low Emission Zones (LEZ) have emerged as one of the most popular mechanisms to tackle urban traffic congestion and its subsequent impact on the environmental pollution. The concept of LEZ, which first appeared in Sweden under the name of "environmental zone" in the late 90s [7], consists of an area where certain restrictions or surcharges are applied to drivers in accordance to their vehicle emissions category. The rapid proliferation of LEZs through all Europe[1] is testimony to governmental administrations' trust in this approach. Central-Europe countries like Germany, The Netherlands, Belgium, the United Kingdom and the north of Italy are clear examples of this increasing trend. Also other countries, that to date are not implementing LEZs, are considering them as a way to honour the Paris Agreement[2]; some of them even by law as the draft bill on Climate Change and Energy Transition of the Spanish Government, that stipulates LEZs as mandatory for cities with more than 50,000 inhabitants[3].

A critical element of this mechanism is the access control system that must be deployed in order to enforce traffic restrictions that a LEZ poses. Currently deployed systems use two main ways of monitoring the compliance of vehicles in the LEZ, one operating in manual way and another based on automated systems. The first implies authorities visually checking the emission category stickers placed on the vehicles' windshield, while the latter is based on cameras and automatic license plate reading. Although manual systems, being the dominant trend in center Europe, are cheaper and much easier to deploy, this measure's effectiveness varies depending on the number of municipal employees assigned to the task of

[1] Urban Access Regulations In Europe deployment map, http://urbanaccessregulations.eu/userhome/map

[2] Paris Agreement, https://unfccc.int/

[3] Strategic Framework of Energy and Climate: https://www.miteco.gob.es/es/cambio-climatico/participacion-publica/marco-estrategico-energia-y-clima.aspx

visually checking the vehicles' stickers. In that sense, manual approaches can not compete with the efficacy of automated control systems like the ones deployed in London, Stockholm or Singapore.

Among currently deployed automated systems, one of the most cited examples in the literature is the London's LEZ and its controversial vehicle control system [8]. The center of London has operated as a LEZ since 2003 and it currently establishes fixed toll rates, weighted by potential CO2 emissions, to all vehicles circulating the restricted area. In order to keep track of those vehicles, the LEZ implements a control system which is composed of a large set of Automatic Number Plate Recogition (ANPR) cameras (approx. 1000) distributed over the London downtown. With this camera network, the system is able to identify the license plates of vehicles for, later, determining if its owner is paying the corresponding monthly fee. Notwithstanding all this infrastructure deployment, the system only guarantees a reasonable probability of dishonest driver detection. A further shortcoming is the false positives generation owing to the accuracy of the ANPR system. The revision of such cases generates personnel and management costs of approximately 130 million pounds[4] every year. Stockholm charging scheme[5] is another example implementing this same approach but differing in the camera network layout. In London's scheme this network spreads over the whole restricted area, contrary to the Stockholm one, in which cameras are placed only in entrance and exit points.

Another much-quoted LEZ example in the literature is the so-called Electronic Road Pricing (ERP) implemented in Singapore. The ERP is a toll-based access control system which restricts the entrance to Singapore's central business district. This system is composed of large infrastructures,

[4] Road Pricing in London, Stockholm and Singapore, http://nyc.streetsblog.org/wp-content/uploads/2018/01/TSTC_A_Way_Forward_CPreport_1.4.18_medium.pdf

[5] Stockholm charging schemes, http://www.stockholm.se/trangselskatt

located in every access road to the restricted zone, which implement all needed mechanisms to identify users and collect tolls. In order to interact with ERP validation infrastructure, the users of the system must purchase a specific transmitter device and integrate it on their vehicle. Toll fees are automatically charged when vehicles drive by an access point thanks to an ad-hoc debit card used by the transmitter devices. System's infrastructures are also embedded with ANPR cameras for enforcement, so vehicles can be identified even if they try to commit fraud in any way. Even though Singapore's scheme has proven to be more effective than the one deployed in London, its implementation is far more complex and not suited for most of cities roads due to the dimensions of the required infrastructures.

As the aforementioned examples reveal, all current automated LEZs share a common problematic as they rely on access control systems based on camera networks, whose purpose is to indiscriminately photograph the license plate of vehicles circulating around the LEZ. This photos are later used to identify those vehicles and to verify their corresponding payments. In any case, these approaches are of an intrusive nature as users will be identified and tracked each time they drive nearby a LEZ's infrastructure. This gathering of information by a centralized entity poses serious privacy issues for those who interact with the system and reveals the need of alternative LEZ control systems which are friendlier to user's privacy. Furthermore, even though these approaches have shown to be feasible on their respective environments, their implementation on a practical level require numerous dedicated infrastructures, incurring in expensive deployment and management costs. The design of secure and reliable schemes that automatize the vehicle access control process while reducing the implantation costs has also become a technological challenge concerning LEZs.

Besides these privacy issues, structural improvements have also been identified in LEZ access control systems due to the strong dependence on centralized entities to manage the processes related to vehicles' access acknowledgment and fee payment. The presence of those centralized entities poses a single point of failure in whole system, endangering its security and availability.

Recent decentralized protocols, built on blockchain technology, can be applied to settle transactions between vehicles and LEZ infrastructures without the involvement of trusted third parties, putting an end to the hegemonic position these centralized entities hold. Nevertheless, the use of a public ledger brings new privacy challenges to the field, as any published transaction fall into the public domain and, thus, driver information contained in these transactions should be accordingly protected.

1.2 Contributions

The implementation of LEZs in urban areas involves applying restrictions or surcharges to vehicles according to their emissions. On that basis, the need of automatized access control systems able to enforce such traffic restrictions have become a critical issue, and fuelled the appearance of novel systems trying to address the invasive nature that current deployed systems present. Nevertheless, the current state-of-the-art works still show serious privacy threats due to the indiscriminate use of camera networks and the centralization of trusted entities. In this thesis, three access control systems for LEZs are presented in order to tackle the identified privacy and functionality conflicts found in the literature.

In the first proposal, we contribute with a new lightweight, secure and privacy-preserving solution for delivering access control to LEZs in which the cornerstone is its deployability in real scenarios. This approach makes use of the driver's smartphone to validate their access instead of relying on an On Board Unit (OBU) thanks to the use of widespread technologies, and, due to a lightweight protocol, it can be run in single-board computers which open a door for a more low-cost system infrastructures. Furthermore, it provides a non-probabilistic fraud control system that always preserves the privacy of honest users, while punishing those who alter or skip parts of the protocol to commit fraud. As a result of the secure access process, the system is also able to obtain metadata which contain information about the vehicles' entries and exits in the LEZ in real time. The inconsistencies within these data shall serve to uncover fraud among the users. This information can also be used by the infrastructure manager to characterize and optimize the access to the LEZ.

Our second contribution introduces a new privacy-preserving approach where third parties are omitted from payment processes in favor of a decentralization that blockchain technology offers. Under this premise, every access to the LEZ is considered as a transaction and, through smart contract interaction, it is published into the blockchain. In the same way, according to the transaction's uploaded access parameters, the blockchain-supported smart contract automatically charges the corresponding fee amount in terms of digital tokens, i.e. elements acting as native currency in our system. Under this procedure, entities responsible of registering vehicle accesses and charging their corresponding fees are replaced by a decentralized network, which grants the verifiability, reliability and transparency of the uploaded events. On this basis, there is no need for entities to locally store signed proofs of every interaction they made, as any node belonging to the distributed network can verify the validity of the transaction flow in the blockchain. Taking this approach, however, has no impact in the inherited privacy model from our first contribution and keeps preserving fraud control system with revocable anonymity.

Finally, in the third contribution, our scheme defines a new decentralized privacy-preserving access control system for LEZ*s* in which user's anonymity is achieved through a tailored group signature scheme, outstanding for its lightweight signature process and not requiring key regeneration to preserve unlinkability. Under this premise, users generate access evidences, signed on behalf of their vehicle emission category group, without disclosing their identities or permitting linkage between them. This is achieved even if these evidences are published in a public ledger like a blockchain on a decentralized model as proposed on our second contribution. With this privacy-preserving scheme, user's anonymity is truly preserved without the need of client-on-demand credentials renewal process, which, due to their computational load, can interfere with critical real-time phases of the protocol.

1.3 Structure of this thesis

The remainder of this thesis is organized as follows. First, in Chapter 2 the existing schemes suitable for LEZ access control enforcement are surveyed. Chapter 3 presents our first contribution, a lightweight LEZ access control system focused on deployability and the use of widespread technologies. The second and third contributions are presented in Chapter 4 and Chapter 5 respectively, presenting two access control protocols for LEZs addressing the centralization problems in fee ascertain processes and the privacy challenges that decentralized public ledgers entail to the field. Finally, the concluding remarks and some guidelines for future research are given in Chapter 6.

Chapter 2

Related work

The introduction of LEZs in heavily populated areas have elicited the need to implement automated access control systems enforcing the restrictions and surcharges that these areas promote. Systems such as those deployed in London, Stockholm or Singapore appeared overtime in order to impersonate this critical element. Although current deployed approaches proved to be effective, the increasing concern of society for individuals' privacy gave rise to criticism to the intrusive nature of currently deployed systems. In response to those claims, several more privacy preserving schemes have recently been proposed [9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19], following an evolution over the years from full vehicle tracking through the indiscriminate use of cameras to only identifying those who ignore the system's protocol.

On this basis, current published approaches allow a clear classification according to the conditions on which they use camera networks to collect vehicles evidences. On one hand, some approaches support the principle of an indiscriminate shooting anti-fraud system in which their infrastructures, acting as checkpoints, take photos of every vehicle's licence plate, permitting the SP to validate the vehicle provided data. On the other hand, more recent schemes in the literature take a different approach based on users' honesty, which only photographs vehicles when a short range communication protocol with the infrastructures is omitted or not successfully completed.

2.1 Indiscriminate evidence collector anti-fraud system

The initial privacy-preserving approaches that appeared in the literature [9, 10, 11, 12, 13, 14] rely on the principle of vehicles gathering fee-relevant data, through the use of their On-Board-Unit (OBU), while circulating inside the restricted area. Then, on the basis of these data, their transit inside the LEZ is priced and sent to a centralized third party, usually a Service Provider (SP), who acknowledges the whole process and charges the required fee.

Even though all these approaches share several features, they can mainly be generalized in two groups according to the way they compute the information related to their traveled path. In the first group, the SP calculates, for each billing period, the corresponding fee to pay from the path information the vehicles' OBU provide. Works in [9] and [10] are clear examples of this approach. Conversely, in the second group, it is the OBU who locally calculates the fees and sends them to the SP as a unique sum in each billing period. Proposals in [11, 12, 13, 14] are examples of this kind of system. It should also be noted that in works using this model, minimum information about the geographic location of the vehicle is disclosed. However, the use of cryptographic evidences is needed in order to prove that the OBU has been honest during the fee calculation process.

In [9] the authors presented VPriv, a system to compute functions over traveled paths for several vehicular location-based services while protecting users' location privacy. The authors make use of several cryptographic mechanisms like secure multi-party computation, homomorphic commitments and zero-knowledge proofs in order to design an efficient protocol for toll charging, speeding detection and “Pay-as-you-go" insurance premiums that preserve the privacy of the drivers. In VPriv, vehicles send time-location tuples together with randomly generated commitment tags, selected beforehand, to the SP at every period of time. The server then calculates all location fees and sends them back, so each user, according to her tags, can compute her location fees to obtain the aggregated fee amount. Later, using a zero-knowledge proof, the user should demonstrate to the server the summation's correctness by answering correctly to a series of challenges. This process, called round protocol, should be run several rounds to avoid users deviating from the system. Furthermore, to ensure the users are not committing irregularities and the computation function is receiving complete and correct data, VPriv also introduces an anti-fraud mechanism to resist physical attacks by means of sporadic random camera-based spot checks. In this process, the authority randomly observes the physical location of cars generating license plate, location and time tuples. Then, during the payment phase, drivers are challenged to prove that some of their data tuples are consistent with the spot check records. This enforcement scheme became a cornerstone for this kind of systems and was adopted by every further OBU-gathering-based approach [10, 11, 12, 13, 14] until a novel paradigm was proposed in [16].

The work in [10], and its extension in [20], proposes another system which follows the same design principles as in VPrip [9], processing the vehicles' location data on the system's server, but built on the basis of group signature scheme in order to preserve the user's privacy and to achieve a better balance between privacy and system's overheads. According to this proposal the vehicle's OBU computes location tuples during the driving phase, composed by locations and time, and, periodically, sends these tuples to a centralized server among with their corresponding group signatures. During the billing period, each user calculates her total aggregated fee according to the public charging policy and the local record of her own location tuples. Then, the total amount is sent to the server, who collects all the users' fees. On its side, the server calculates the total fee to pay for each group using all the received tuples. In case that some mismatch is detected between the server calculation and the amounts sent by the members of that group, a dispute resolve phase is initiated. The group authority is who receives any fraud claim and determines who the misbehaving participants are. To do this, the authority opens the location signatures, received from the server, and computes the real toll fee for each user in this group; in this way it can determine which users are committing fraud. Still, the users can demonstrate their innocence by sending their stored proofs, signed by the server, and prove to the authority that the server is the one who is misbehaving. Either way, even with the assumption that OBUs are tamper-proof, reliable, trustworthy and configured by a trusted authority, this approach is still vulnerable to physical attacks and, as the authors state, an anti-fraud system based on camera-embedded spot checks like in [9] is needed to overcome this vulnerability.

PrETP was proposed in [11] considering a different approach, in which vehicles' OBUs locally compute their fees according to their traveled route, while disclosing the minimum amount of location data to the SP. During the driving phase, the OBU calculates the subfees corresponding to their trajectories according to the SP pricing policy. Then, at the end of each billing period, the OBU aggregates all the subfees and sends them to the SP as a total amount, safeguarding the user's privacy from the SP and any other third party eavesdropping the communications. PrETP employs a cryptographic protocol, called Optimistic Payment, as an enforcement mechanism for the correct fee calculation on the driver side. According to this protocol, OBUs send commitments, which do not reveal sensitive information to the SP, of the locations and prices used in the fee computation along with the final aggregated fee. In order to check the veracity of the committed values, the SP, who is able to obtain physical proofs of vehicles via camera-based spot checks as proposed in [9], challenges the vehicle's OBU to prove that it was at the location the photo reveals. To this end, the OBU opens the commitment containing this specific location and proving to the SP the correctness of the fee aggregated data, thus revealing only the location and price data at the instants of the challenged proofs.

In [12], the authors identify drivers collusion as a potential threat in the security of PrETP and any other scheme using the spot check enforce system proposed in [9]. In this attack, as spot checks are leaked during the reconciliation phase, drivers may collude to map and share their known camera locations, and, on that basis, only send correct travelled tuples when they are nearby to a spot check. In order to tackle this flaw, the authors propose Milo, a system designed as an extension of PrETP that makes use of blind identity-based [21] encryption to avoid revealing the spot checks' location during the monthly reconciliation phase. However, the location of spot checks is still revealed when a photo is taken to identify a dishonest driver.

SPEcTRe, another improvement of PrETP, was presented in [13]. The authors propose a system based on RSA blind signatures in which e-cash [22] was first used to pay the driving fees. In SPEcTRe, users buy a set of pre-generated tokens, signed by the service provider, which are bound to their vehicle license plate. During the driving phase, the drivers spend tokens by broadcasting them. In order to ensure that drivers are honestly following this procedure, a spot check system monitors drivers at random locations and times. In this monitoring process, spot checks take a pictures of the vehicles' licence plate along with the tokens they are broadcasting. Finally, during the payment phase, drivers submit to the payment server all unused tokens to redeem them and pay for the ones that were used. The payment server verifies that non of the submitted tokens were captured by its spot check enforce system in order to ascertain that the users are not committing fraud.

A different approach based on cells was presented in [23, 14]. In this scheme, the restricted area is divided into little fixed parcels, called cells, which represent the basic unit for determining the fee calculation of the vehicles. Of all the cells an area is divided, a certain amount of them are selected as spot check cells and are equipped with a camera to operate as an enforcement system. While driving, the OBU provides to its Secure Element (SE), which knows the selected spot check cells, the current location and time when the vehicle enters a new cell. The SE updates the total toll and generates a proof of participation, which contains encrypted data under the SP's private key when the vehicle is inside a spot check cell. During the reporting period, the SP opens the tickets from the spot checks cells where the vehicle was photographed and verifies the validity of their content. On that basis, the SP can determine the honesty of the aggregated fee the user submitted.

As the above-mentioned works reveal, all systems relaying on client-side's OBU for gathering fee-relevant data are susceptible to fraud strategies based on physical attacks like, for example, modifying the OBU's data flow or shutting the OBU down. In order to ensure the drivers are not committing irregularities and the OBU is managing complete and correct data, these systems share a common anti-fraud mechanism, introduced by [9], based on sporadic spot checks. As aforementioned in this section, the basis of this anti-fraud system is to indiscriminately register the physical location of cars through the recording of their license plates by means of camera-based checkpoints. These recordings are proof of the real location of the vehicles at a particular time and could show whether the traveled data of a vehicle has been altered or the OBU has been turned off. In that respect, users are challenged to generate cryptographic proofs supporting that their data are consistent with the gathered license plate records.

In the light of the conclusions drawn from [12], this anti-fraud strategy relies on the wrong assumption that spot checks are unpredictable. Spot checks are physical infrastructures composed at least of a camera and a transmission device, which could be easy to identify and difficult to relocate. Therefore, this fraud detection system has a certain failure probability that directly depends on the number of spot checks deployed in the restricted area. In this manner, drivers could take advantage of this flaw, e.g. deliberately bypass spot checks or just turn the OBU on in these points, and continue committing fraud. Increasing the number of spot checks is usually the default strategy to overcome this situation and detect fraudulent users with a greater probability, posing a trade-off between user's privacy and fraud detection. Nevertheless, implementing this strategy not only negatively compromises the user's privacy as their location is more often registered, but also could enable the SP to track vehicles all by itself without needing the OBU's information to estimate users' fees.

2.2 Conditional evidence collector anti-fraud system

In the recent years, a new paradigm has taken hold since it was proposed in [16] and later adopted in [17, 18, 19]. This new model is focused on user's privacy and promotes that users' anonymity is always preserved unless they try to commit fraudulent actions. In this matter, systems using this paradigm only take photos of vehicle's license plates in case a short range authentication process with the system's infrastructures is not completed or totally omitted.

The system presented in [15] and its further extension in [16] introduces, besides the aforementioned anti-fraud paradigm, a privacy-preserving access control protocol for LEZs based on a time approach, where fees are computed according to the users' elapsed time inside the LEZ. In this scheme, during the driving phase, vehicles communicate with the spot checks placed at the entrances and exits of the LEZ and authenticate each other through their public key certificates. From this interaction, both entities receive a proof-of-entrance and proof-of-departure signed by the counterpart. If at any point an authentication process fails, the spot check takes a photo of the vehicle's license plate, thus, generating a fraud incidence proof. During the payment phase, each driver computes their entrance and departure recipes and directly prices, in terms of elapsed time and vehicle category, and pays his access using some anonymous and untraceable e-cash scheme. As a result of the payment process a payment receipt is obtained and sent to the SP. Later, during the billing period, the SP verifies that each payment receipt is in accordance with entrance and departure proofs and opens an incidence if required.

The authors in [17] improve the former scheme to dynamically change the fees of a set of LEZ's subsets, called stretches, according to their traffic density. In this manner, the price increase on dense traffic areas would motivate drivers to avoid them and choose alternative routes. Therefore, it could be assumed that a better traffic management could be achieved by controlling the flow and the density of vehicles in the different areas resulting in a reduction of traffic jams. In this scheme, the restricted area is divided into a set of one-way sections of streets, called stretches, where a fee should be paid each time a vehicle drives through it. When a vehicle enters the payment area of a stretch, a beacon sends the prices, set by the SP, for that segment and the required fee is calculated in terms of the received prices and the vehicle's emission category. Then, the driver makes the corresponding payment to a trusted Payment Service entity and receives a proof-of-payment when it is completed. This proof-of-payment is then sent to a Ticket provider, controlled by the SP, to obtain an access ticket for the current stretch. When the vehicle reaches the current stretch's spot check, it authenticates and sends the obtained access ticket. The spot check, then, verifies the access ticket validity and sends a proof-of-entrance back as a receipt. If at some point the authentication or the verification processes fails, the spot check takes a picture of the vehicle license plate as an evidence of fraud. While the vehicle remains in the LEZ, the whole process is repeated each time a new stretch is accessed.

In both protocols [16, 17] the users' privacy is protected by means of pseudonyms and a group signature scheme. In this setting, each user's OBU has a pre-configured secure element containing a *Certification Authority* of the group she belongs to, allowing her to regenerate her key pairs and public key certificates. This way, the users regenerate their keys and certificates after each access to the LEZ to avoid their traceability through their signatures. Furthermore, the users' certificates do not contain users' information on them in order to prevent their identification, and include the users' identifier probabilistically encrypted with the public key of a trusted party to be able to revoke their anonymity in case of fraud.

These two works [16, 17] provide an alternative approach to tackle the lack of privacy-preserving solutions in the literature; however, both proposals incur in significant run time costs due to the nature of those solutions, which perform several costly operations linked to a complex payment procedure and the cryptographic key material regeneration steps. Furthermore, these two schemes require an ad-hoc OBU and permissions to access its functionalities. The fact that the integration of OBUs in current vehicles is not widespread, and that most of their functionalities are restricted for third-party applications, represents two significant shortcomings for those methods that undoubtedly limit their effective deployability in a near future.

In [18] the authors designed an electronic road pricing system built around a building-block digital wallet called black-box accumulation or BBA+, introduced in [24], which provides the core functionality of keeping a balance while providing unlinkability. In their protocol, every time a user goes through a system's infrastructure, the Debt Accumulation phase is executed. During this phase, the user fee is determined and the corresponding debt is added to her wallet, along with some public attributes of the infrastructure. The toll can be dynamic and dependent on factors like the user's attributes attached to the wallet, the traffic congestion or the last met infrastructure. During this phase, commitments and non-interactive zero knowledge proofs are used to update the wallet to its next state, preventing users from using previous states of the wallet with less accumulated debt to commit fraud. The infrastructure's camera takes a photo of the vehicle's license plate in case of protocol omission or failure, so further action can be taken against the fraudulent user. At the end of the billing period, users send their wallets to the SP in order to clear their accumulated debt. The SP, who in advance knows to whom each wallet belongs, invoices each wallet and checks if its user has physically paid the corresponding accumulated amount. Once the debt clearance is completed, the wallet in invalidated and the user asks the SP to create and bind a new wallet to her account. Also during the billing period, the SP receives entries of every Debt Accumulation interaction from the system's infrastructures and runs the Double-spending protocol. By means of this protocol, the SP is able to detect and identify, among all the Debt Accumulation entries, those users consuming previous states of their wallets to commit fraud.

In this scheme [18], the authors propose a use case for the digital wallet they introduced in previous works. In the proposed system, built around the unlinkability property their wallet provides, privacy is preserved by distributing the driver's data among different system's entities and assuming the risk of collusion. Nevertheless, as the authors state in their article, the SP stores information of every Debt Accumulation interaction between vehicles and system's infrastructures, containing non-identifying attributes of both entities. These attributes along with some background knowledge, e.g. infrastructures' geo-position and the road distribution, could be used to find a path such that the sum of the prices of the transactions on this path equals the total balance of the user's wallet. In the end, the authors conclude that the more detailed these attributes are, the easier is to find a single solution to this problem and, therefore, jeopardize the user's privacy. Another point to improve, also stated by the authors, is the privacy revocation of honest users if the Debt Accumulation phase is aborted prematurely, even if the cause is beyond the user's control. In this case, when a user is not able to correctly update her wallet to its new status, due to any technical or communication problem, she is forced to start the next interaction from the same status as before. Thus, the double-spending detection mechanism will identify her as dishonest user, disclosing her private key and, therefore, unveiling her identity.

The work in [19] proposes another approach to compute functions over the traveled distance registered by the vehicles' OBU, which integrates the anti-fraud principle of always preserving the users' privacy unless they try to commit fraud introduced in [16]. According to this proposal, the vehicle's OBU transmits geolocation tuples to the SP each time it meets a Road-Side Unit during the driving phase. The users' privacy is preserved during the whole process by means of pseudonyms and credentials renewal. The main contribution of this work, however, is its anti-fraud scheme, which turns the vehicles circulating inside the restricted area into mobile spot checks. The proposed approach is based on the vehicle-to-vehicle (V2V) communication process, the obstacle detection system and the camera embedded in new generation cars. When a vehicle's sensors detect another car, a V2V communication is initiated and, in case of no response, a fraud case is assumed as the no responding vehicle may have its OBU turned off. In that case, the vehicle takes a photo of the fraudulent user's license plate and transmits the information to the SP via road-side unit. Finally, during the tolling period, the SP computes the total fee to pay for each driver according to the sent geoposition tuples and initiate measures against the registered fraud cases.

This work in [19] presents an anti-fraud system, validated in a simulated scenario, where users collaborate to act as checkpoints; nevertheless, the scheme is built on the wrong assumption that shutting the OBU off, ceasing all interactions with other entities, is the only way for the users to commit fraud. On this basis, a user denying every communication with Road-side units while responding to V2V challenges from other vehicles could bypass the system and not be detected as fraudulent, since Road-side units do not receive any information about the vehicles responding to V2V challenges. In addition to that, the SP, as a fee charging entity, holds a favorable position over the users, knowing all their geolocation tuples and being able to link all their pseudonyms. As users generate their pseudonyms in conjunction with the Road-side units, the SP, owner of these infrastructures, is able to obtain such information. This inherent omniscience allows the SP to link all users' actions inside the restricted area and, therefore, jeopardizes their privacy.

As it can be inferred from current works in the literature, on top of each individual scheme's issues, common structural improvements can be identified in LEZ enforcing systems due to the strong dependence on centralized entities, usually an SP, to acknowledge vehicles' access data, ascertain their traffic fee and charge its corresponding amount of money. This way of proceeding places centralized entities in a dominant position posing a potential single point of failure, which makes the whole system more vulnerable to technical failures and malicious attacks threatening its security and availability. Furthermore, the mechanisms to address this problematic require the settlement of transactions between vehicles and system infrastructures through the mediation of decentralized public ledgers. The publication of data in that kind of ledgers entails, however, new privacy, traceabiliy and linkability challenges to the field, as the uploaded information falls into public domain and should be accordingly protected.

Chapter 3

Secure and Privacy-Preserving Lightweight Access Control for LEZs

In this chapter we introduce a new access control system for LEZs in order to tackle the identified problematic in Chapter 2, concerning the intrusive nature and the limited deployability present in the current literature works. The objective of our proposal is to offer a lightweight, secure and privacy-preserving system for delivering access control to LEZs in which the cornerstone is its deployability in real scenarios. In contrast to other schemes, it is specially designed to provide effective anti-fraud measures to identify fraudulent users, who alter the protocol for their own profit, while preserving the privacy of the drivers who behave honestly. Furthermore, the lightweight design and the use of widespread technologies permit its implementation in low-cost infrastructures and the use of smartphones as client-side devices. On the basis of this implementation, we present experimental results that validate that our system's feasibility in relevant scenarios as defined in TRL5 level of technological maturity.

The contributions in this Chapter have been published in [25] and an extended version of this work has been published in a journal in [26].

The remainder of this Chapter is structured as follows. Section 3.1 introduces the model of the system giving an overview of the proposal. Section 3.2 describes the proposed system and the protocol on which it is based. Section 3.3 provides a security and privacy analysis. Finally, Section 3.4 presents an extensive evaluation of the proposed scheme, including details about the implementation and the tests done, in both controlled and real environments.

3.1 Preliminaries

In the current literature, the schemes controlling the access of vehicles to restricted areas mostly rely on plate recognition by means of cameras. In the worst case scenario, the plate recognition is used to directly identify vehicles, from which a complete tracking of every user can be performed. More privacy-aware approaches only use plate recognition at certain points to verify the drivers' honesty and counter fraud. Either way, these schemes present two major drawbacks: they are expensive and do not respect the drivers' privacy. On the one hand, the implementation of these systems is expensive, as installation and maintenance of sophisticated cameras and Optical Character Recognition system (OCR) are required. On the other hand, they are disrespectful with their users' privacy as, at some point, all those systems use license plate recognition to identify the drivers who are traveling inside the restricted area, whether they are honest or not.

Our scheme uses a different approach whereby the communication between the infrastructure and the user is only established during the entrance and exit from the restricted area, without the need of random-located spot checks to identify users. Furthermore, the users' privacy is always respected as long as they follow the protocol and terminate the communication with the infrastructure correctly. Otherwise, users are identified and fined. In our system, communication is achieved via widespread technologies (WIFI, Bluetooth Low Energy, Bluetooth, etc.) so any current Smartphone can be used to interact with the infrastructure. The use of widespread technologies together with a lightweight authentication protocol makes it possible to run our scheme in single-board computers, which results in small and low-cost infrastructures.

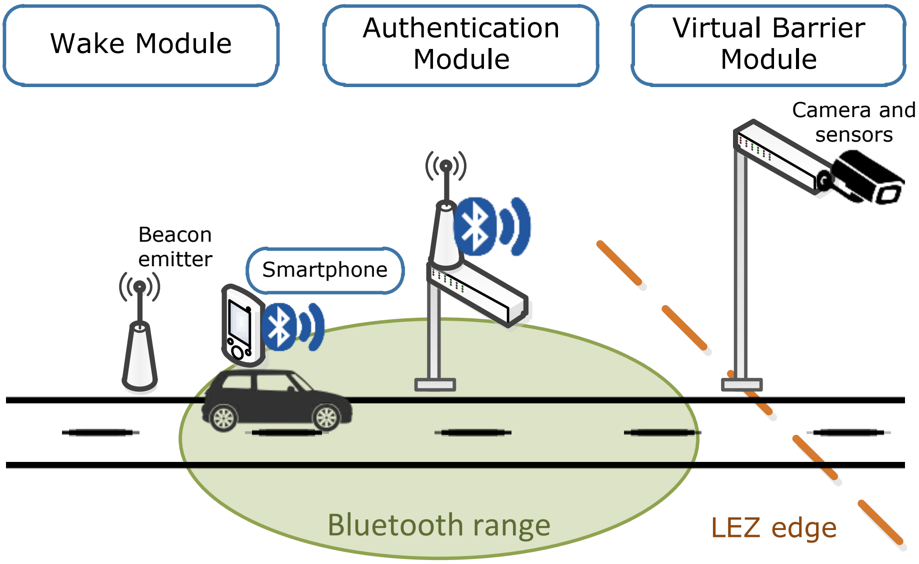


Figure 3.1: Access infrastructure

Figure 3.1 represents a general scheme of the proposed LEZ access control system. In this scheme, two entities are involved: the Access Control (AC) infrastructure and the user's Smartphone. The AC entity is divided in three physical independent modules according to their function:

(i) Wake Module, which emits beacons to wake up users' smartphones; (ii) Authentication Module, which communicates with users' smartphones and validate their accesses; and Virtual Barrier Module, which detects vehicles and takes plates photos when validation process fails. Such deployment was proposed to easily relocate those modules and, therefore, be able to make the maximum advantage of the range of the omnidirectional communication device built-in in the Authentication Module. In order to interact with the system infrastructure, it is required that the driver has registered and validated her information to the Competent Administration of the LEZ, and has installed and configured the mobile application into her Smartphone. During this configuration, the user must register and validate her vehicle in order to determine its vehicle emissions category.

When a vehicle approaches a LEZ access or exit area, the driver's smartphone awakes the mobile phone application once it detects a signal from the Wake Module. This process is automatically done without any intervention from the driver. Then, the mobile application establishes a secure communication with the Authentication Module and initiates the cryptographic protocol in order to prove that the user is driving a valid registered vehicle. Due to the use of pseudonyms, which can be changed at user's request, the anonymity of the driver is preserved during the whole process. Through the resolution of the protocol, the AC entity is able to determine whether the credentials of the user's vehicle are correct or not.

The user can proceed to the LEZ preserving her privacy if her credentials turn out to be valid. It should be noted that the access and exit information is stored in order to calculate the users' fees according to the emission category of the vehicles she used. Conversely, if the user fails to complete this protocol phase in any way, the Virtual Barrier Module of the AC, which physically determines the end of the authentication area, will take a photo of the vehicle's license plate. The photo will serve to identify the dishonest user and, thus, revoking her privacy.

In a nutshell, the proposed scheme meets a set of operational and competitive advantages over traditional systems:

- Revocable anonymity: The users' privacy is guaranteed, as long as they behave correctly. In other words, the system should not be able to identify an honest user which has valid credentials. Conversely, the identity of dishonest users who do not follow the protocol or have invalid credentials should be disclosed.

- Widespread technologies: The use of widespread communication technologies like Bluetooth, BLE or WI-FI makes possible that a large number of devices meet the requirements for interacting with the system's infrastructures. In this way, users can make use of their own mobile devices to communicate with the infrastructure instead of purchasing an ad-hoc device for this purpose.

- Reduced infrastructures: The lightweight nature of the presented cryptographic protocol enables that single-board computers can be used to run our scheme in a reasonable amount of time. Consequently, the infrastructures can be built with reduced size and, therefore, be easily integrated in different urban environments. Furthermore, this also results in a low building, operating and maintenance costs.

- Metadata: the AC can recollect anonymous mobility data from the vehicles that enter and leave the LEZ. The aim of this mobility data is to extract, through its analysis, useful information that can be used for future planning and managing of the LEZ.

3.2 Our proposal

In this section, actors involved in proposed scheme are introduced in the first place. Secondly, a thorough description of all protocol's phases are presented.

3.2.1 Actors

Figure 3.2 shows the actors involved in the presented system: i) Competent Administration of the LEZ (*LA*); (ii) Drivers (*D*); iii) Service Provider (*SP*); v) Vehicle Binding Device (*VBD*) and; iv) Fraud Control (*FC*). The LA is the entity in charge of managing the LEZ. Among its tasks it is responsible for setting the access rules, the price, and charging the accesses to the drivers. For example, it can set different LEZ's aspects such as setting a special rate for residents, establishing a fee per access, or establishing an annual, monthly or weekly rate. The vehicle drivers (*D*) are the group of users for which this approach is intended. *D*s should hold a Smartphone with the mobile application installed, configured and running on it in order to interact with the infrastructures of the LEZ. The Service Provider (*SP*) is the entity who carries out the access control to the LEZ and sends the needed information to the *LA* so that it can compute the service pricing. The Vehicle Binding Device (*VBD*) is a little anti-fraud BLE device, which has GPS technology built-in, designed to generate cryptographic evidences in order to proof a bind between the vehicle and the driver's Smartphone. Non-repudiation, integrity, authenticity and non-traceability are properties the generated evidence should grant. It is assumed that VBD will be of a reduced-price, reduced-size and non-removable without ceasing its functioning. The Fraud Control (*FC*) is an entity that, based on the data provided by *SP* and *LA*, identifies unusual patterns that could lead to detect fraudulent users.

It should be mentioned that the SP has a pair of keys of an asymmetric cryptosystem (Pb^{SP}, Pr^{SP}) (Pb^{SP} is the public key, Pr^{SP} the private) and its corresponding certificate Γ^{SP}. The LA also has a key pair (Pb^{LA}, Pr^{LA}) and its certificate Γ^{LA} with the attribute to issue certificates.

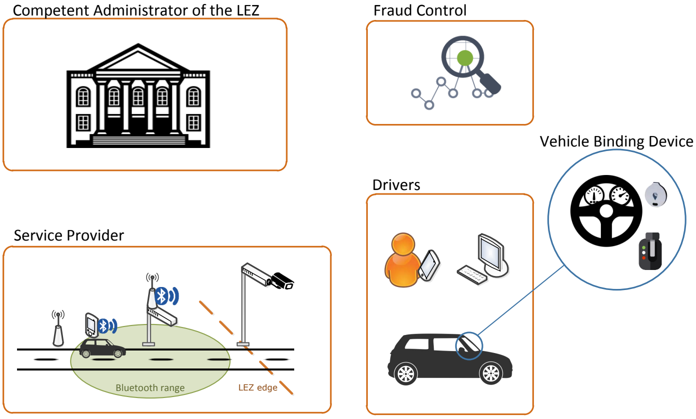


Figure 3.2: System's actors

3.2.2 Phases

The lifecycle of the proposed system could be divided into the following phases: i) Registration; ii) Installation; iii) Vehicle Registration; iv) Access; v) Exit; vi) Payment; vii) Privacy Configuration and; viii) Fraud Control

Register

The first phase the users must complete is the registration in the LA. The users should provide their personal data to the LA and, when this information is validated, they receive a registration code. This code will be needed in the installation phase.

- D accesses the LA website over a secure connection and provides the registration information (name, surname, e-mail, etc.). This process

Table 3.1: Notation

Name	Description	Name	Description
Pb^{SP}	SP's public key	γ	User's certificate Request
Pr^{SP}	SP's private key	ξ	Contract between D and LA
Γ^{SP}	SP's Certificate	β	Vehicle Code
Pb^{LA}	LA's public key	β'	$Hash(\beta)$
Pr^{LA}	LA's private key	α	User Code
Γ^{LA}	LA's Certificate	α'	$Hash(\alpha)$
Pb^{D}	Driver's public key	χ	New access information
Pr^{D}	Driver's private key	σ	Travel direction
Γ^{D}	Driver's Certificate	ρ	Travel date
Pb^{V}	Vehicle's public key	δ	Travel time
Pr^{V}	Vehicle's private key	ω	Access Data
Γ^{V}	Vehicle's Certificate	ω'	Signed ω
τ	Vehicle Emissions Category	χ'	New exit information
γ^{V}	Vehicle's Certificate Request	ω^{*}	Journey data
$\gamma^{V'}$	Signed γ^{V}	$\omega^{*'}$	Signed journey data
μ	Price	ν	Billing period
λ	List of accesses for each β'	η	Amount to pay
Δ	List of Payments	ϱ	List of accesses for each β'
υ	Masked identity	Θ	Masked list of accesses
ID^{VBD}	VBD ID	ψ^{ID}	VBD masked identity
K^{VBD}	VBD's symetric key	ψ	Vehicle binding data
Pb^{VBD}	VBD's public key	$\psi^{'}$	Signed (ψ, ψ^{*}) by VBD
Pr^{VBD}	VBD's private key	$\psi^{''}$	Signed (ψ, ψ^{*}) by D
Γ^{VBD}	VBD's Certificate	$\psi^{'''}$	Signed (ψ, ψ^{*}) by SP
Γ^{FC}	FC's Certificate	ψ^{*}	Vehicle binding proof

also includes fee related data like whether the user is a LEZ resident or not, the payment method (direct debit, credit card, etc.) or the billing periods, i.e. the terms and conditions of the contract ξ.

- LA performs the following operations:
  - Verifies the data provided by the user. In the event that the user is a LEZ resident, this operation may require an additional time.
  - If the information is correct, the LA generates the user code α which consists of a 128-bit pseudo-random value encoded in

base 32.

  - Binds the α code to the user (D) who requested the registration.
  - Sends an email to D containing an URL linked to the user code α. This link can only be accessed once and for a limited period of time (One-Time Secret). If D has not accessed the link when this time has elapsed, she should request the generation of a new code α.

- D, once she has received the email from LA, should store α code as it will be needed to complete the installation phase.

Installation of the mobile application

When the user D has completed her registration in the system, she can proceed to install the mobile application on her smartphone. This installation cannot be completed without a valid α code.

- D carries out the following actions:
  - Generates an asymmetric cryptosystem key pair (Pb^D, Pr^D). The key pair is securely stored into the user's smartphone.
  - Calculates $\alpha' = Hash(\alpha)$, where $Hash$ is a cryptographic digest function that is considered secure.
  - Generates a certificate request γ from (Pb^D, Pr^D). The field **CommonName** contains the previously calculated α' attribute, i.e. it does not contain any user's personal data.
  - Establishes a secure communication channel, via TLS, with the LA entity and sends the code α and certificate request γ.
- LA performs the following operations:

- Verifies the following points before proceeding with the installation: i) α code is in its database and is valid; ii) the **Common-Name** field equals to $Hash(\alpha)$ and; iii) the certificate request is valid.
- If the previous verifications are successful, it issues the certificate Γ^D. The validity period can be established according to the agreement (ξ) with D.
- Sends Γ^D to D.

- D verifies Γ^D through Γ^{LA} and securely stores it.

Vehicle registration

Upon D has correctly installed and configured the mobile application, she can proceed to register any vehicle she would like to use for accessing the LEZ. Figure 3.3 illustrates this process.

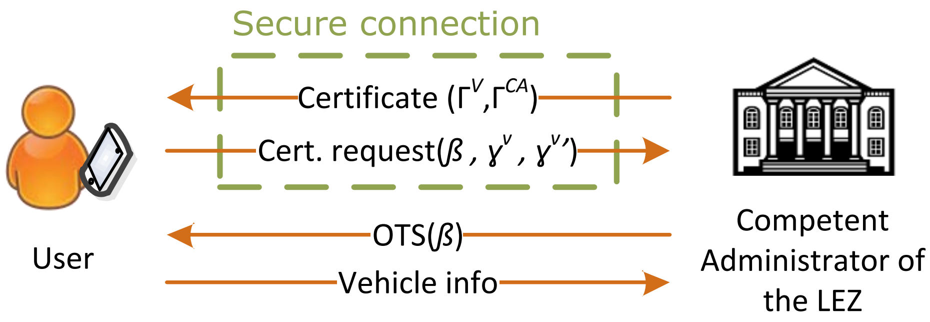

Secure connection
Certificate (Γ^V,Γ^CA)
Cert. request(ß , γ^v , γ^v')
OTS(ß)
Vehicle info
User
Competent Administrator of the LEZ

Figure 3.3: Vehicle registration phase

- D starts the mobile application and initiates the vehicle registration process providing the following vehicle information: plate number, car maker, model, etc.

- LA performs the following operations once it has received the information:
    - Verifies if the provided vehicle data is consistent with the plate number and if the user is the vehicle owner.
    - If the previous verifications are successful it does the following steps: i) generates a vehicle code β which consists of a 128-bit pseudo-random value encoded in base 32; ii) binds the vehicle code β to the user D and; iii) sends an email to D containing an One-Time-Secret (OTS) URL linked to the vehicle code β.
- D, once she has retrieved the β code from the OTS link, carries out the following actions:
    - Generates an asymmetric key pair (Pb^V, Pr^V) for the registered vehicle and securely stores them.
    - Calculates $\beta' = Hash(\beta)$.
    - Generates a certificate request γ^V from (Pb^V, Pr^V). The field **CommonName** contains the previously calculated β' attribute.
    - Calculates the digital signature of the certificate request γ^V with Pr^D obtaining $\gamma^{V'}$.
    - Establishes a secure communication channel with the LA and sends the following information: β, γ^V and $\gamma^{V'}$.
- LA performs the following operations:
    - Verifies the following points: i) β code is in its database and is valid; ii) the **CommonName** field equals to the $Hash(\beta)$; and iii) the certificate request γ^V and its digital signature $\gamma^{V'}$ are valid.
    - Continues with the following steps if the previous verifications are successful, otherwise aborts the vehicle registration.

  - Stores γ^V and $\gamma^{V'}$. We should note that $\gamma^{V'}$ binds the vehicle with D.
  - Issues the certificate Γ^V. The vehicle emissions category τ is included in the certificate as an extension (X509 v3). The LA can include another extensions, for example a link to the ξ, or if D lives in the LEZ.
  - Sends the generated certificate Γ^V to D.

- D carries out the following actions:
  - Verifies the validity of the received certificate Γ^V through Γ^{LA}.
  - If the previous verification is correct, Γ^V and (Pb^V, Pr^V) are securely stored.

Vehicle Binding

Due to the vehicle-emissions-based tolling of the proposed system, a way to verify the emission category of the car the users are driving is needed. Bearing this in mind, the FC configures raw VBD devices to securely issue vehicle binding evidence. The LA is responsible to install this anti-fraud measure before a user can access to the restricted area normally.

- The configuration process that FC conducts for each device VBD is as follows:
  - Generates a symmetric key K_i^{VBD}.
  - Generates a new asymmetric key pair (Pb_i^{VBD}, Pr_i^{VBD}) and its respective certificate Γ_i^{VBD} issued by FC.
  - Generates a random unique identifier ID_i^{VBD}.
  - FC stores K_i^{VBD} and Γ_i^{VBD}.

  - The generated elements K_i^{VBD}, Pb_i^{VBD}, Pr_i^{VBD}, Γ_i^{VBD}, ID_i^{VBD}, the FC certificate Γ^{FC} and the vehicle emission category are securely stored in the VBD.
  - Physically sends to LA all the configured devices.

At this point, it is assumed that LA holds stocks of non-removable VBD devices configured for any vehicle emission category. Once the user D has completed the mobile application installation and successfully registered a vehicle, she must obtain a suited VBD for its vehicle's category in an authorized LA center:

- The user D brings the registered car to an authorized LA center.
- LA carries out the following actions:
  - Verifies if the registered data corresponds to the user's vehicle.
  - Verifies (or determines) emission category of the user's vehicle.
  - Installs a VBD accordingly configured to the emissions category of the car.

Access

When D wants to access the LEZ, she establishes communication with AC, which is under control of SP, in order to validate her access to the LEZ. During this process, shown in Figure 3.4, the next steps are followed:

- D carries out the next operations:
  - When the vehicle enters into the BLE range, the LEZ access mobile application, which is running in the background, automatically wakes up. At this time, D's Smartphone sends a wake signal to VBD to state that a vehicle binding proof should be generated.

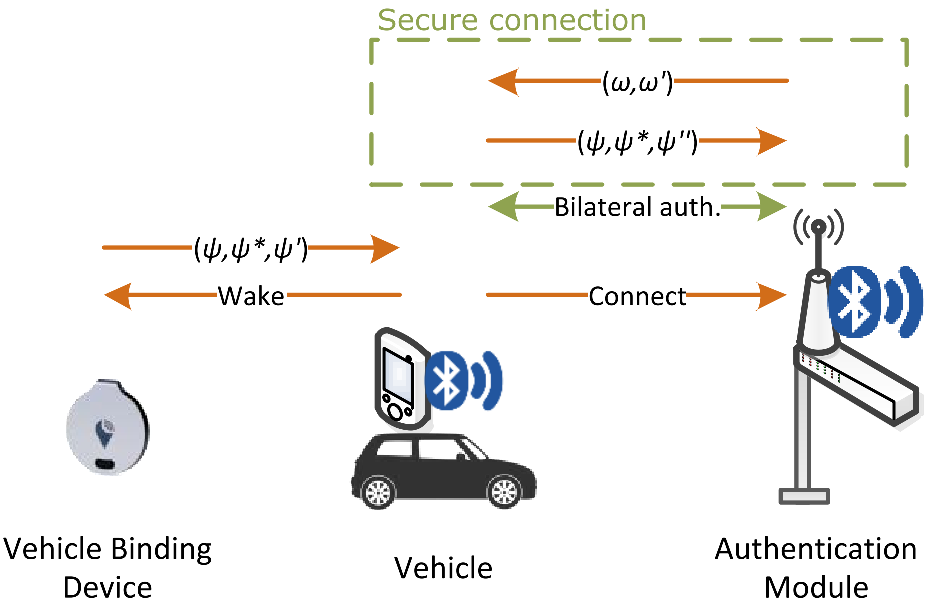


Figure 3.4: Access phase

- In case the user D has more than one vehicle registered, the application loads the vehicle profile the user selected by default. Loading a vehicle profile involves the usage of its key pair (Pb^V, Pr^V) and certificate Γ^V.
- Once the mobile application has automatically started, it establishes communication with the AC entity. The communication comprises a strong bilateral authentication.

- Simultaneously, VBD performs the next operations:
    - Generates a masked identifier ψ^{ID} by encrypting ID_i^{VBD} with RSA_{OAEP} [1] using the FC public key.

[1] OAEP is a standardized padding scheme in PKCS1 v2, which used together with a

- Generates a vehicle binding proof which consist in a cryptographic keyed-hash function ψ^* digested from the data $\psi||ID_i^{VBD}$, where ψ=$\{\psi^{ID}$, position, date, time, $\tau\}$, computed with a symmetric key K_i^{VBD} only known by the VBD and FC.
- Generates the signature $\psi^{'}$ from (ψ, ψ^*).
- Sends the generated vehicle binding proof $(\psi, \psi^*, \psi^{'})$ to D.

- D, once received the vehicle binding proof, performs the following operations:
  - Checks if the received data ψ is correct and verifies the signature ψ' using the VBD certificate
  - If any verification of the previous verifications fails, D notifies the incidence and will be convened to revise her VBD.
  - Stores the tuple $(\psi, \psi^*, \psi^{'})$ as evidence of received data.
  - Generates its digital signature $\psi^{''}$ from (ψ, ψ^*) and replaces the VBD signature ψ' with his own.
  - Sends to AC, by means of the previously established secure channel, $(\psi, \psi^*, \psi^{''})$.

- AC performs the following operations:
  - Verifies that Γ^V certificate is valid and has not expired.
  - Checks if the received data ψ is correct and verifies the signature $\psi^{''}$.
  - Verifies if the Vehicle Emissions Category τ in ψ is consistent with the one included in Γ^V.
  - Stores the new access χ into the database if the previous verifications are successful. It contains the travel direction σ, the

deterministic encryption scheme, like RSA, converts it into a probabilistic one.

date ρ, the current time δ and the vehicle binding evidence $(\psi, \psi^{*}, \psi^{''})$. All this information is bind to its respective user through the vehicle's code β. The vehicle category τ is included in the Γ^{V} used in the authentication.

- Checks the presence sensor and verifies if the detected vehicle has been authenticated.
- If the previous verifications are correct, the vehicle can proceed normally into the LEZ. Otherwise, when the presence sensor detects an unauthenticated vehicle, the system takes a photo of the vehicle license plate.
- Finally, sends the access data $\omega = \{\chi, \beta'\}$ and its digital signature $\omega^{'}$ as a proof of the access to D.

- D verifies the result of the access ω and $\omega^{'}$. The received data is stored as proof of the access.

Exit

In the same way as the access process, the vehicles leaving the LEZ should register their exit. During a vehicle exit the same operations as in the access process are performed. However, AC and D exchange different information to generate the vehicle leaving evidence. Once the bilateral authentication is achieved, both entities exchange the following data:

- D sends a proof and its respective signature of her last entrance to LEZ ω and $\omega^{'}$.
- AC performs the following operations:
  - Verifies if the received access evidence ω and $\omega^{'}$ are valid.
  - Stores a new exit χ' into the database and binds it to the vehicle code digest β'.

  - Sends the exit data $\omega^* = \{\chi', \omega, \omega'\}$ and its digital signature $\omega^{*'}$ as a proof of the vehicle exit to D.

- D verifies the result of the exit process ω^* and $\omega^{*'}$ as proof of the LEZ exit. If the verification is successful stores the information received.

Payment

LA is responsible of charging the vehicle registered accesses for the LEZ. In order to accurately calculate each vehicle fees, it must be provided with the information the SP gathered. It should be noted that all communications are established using a secure channel. The process, illustrated in Figure 3.5 is as follows:

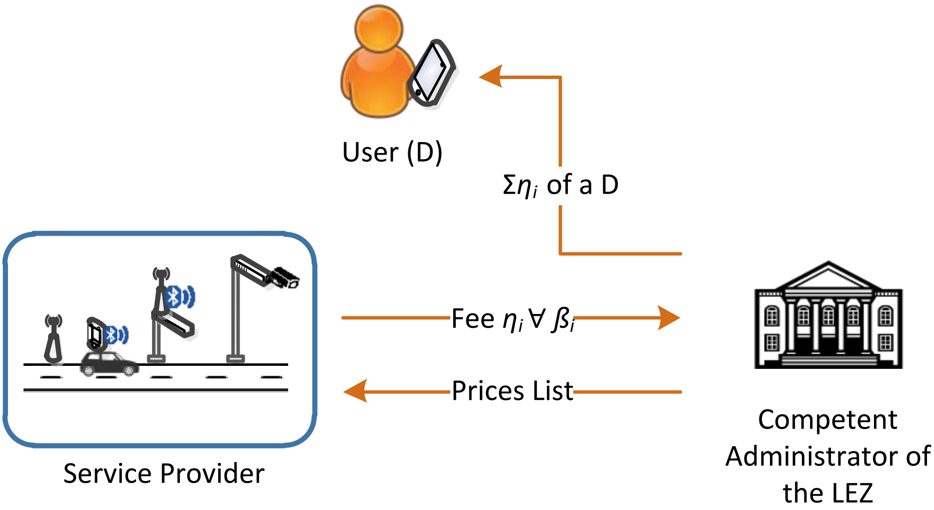


Figure 3.5: Payment phase

- LA sends a list κ to SP with the price μ for each period of time ν and for each vehicle emission category τ_i, $\kappa = \{(\mu_1, \nu_1, \tau_{i1}), \ldots, (\mu_s, \nu_s, \tau_{is})\}$.

- SP performs the following operations:
  - For each vehicle code digest β'_i, it generates a list λ_i containing all the registered access $\lambda_i = \{\tau_i, (\sigma_1, \rho_1, \delta_1), \ldots, (\sigma_m, \rho_m, \delta_m)\}$. We should note that τ_i is obtained from the Γ^V with the **CommonName** field equals to the $Hash(\beta_i)$. In the case the list is empty, the vehicle code digest β'_i is not included. It should also be noted that only the accesses registered since the last billing period are taken into account.
  - Calculates the amount to pay η_i for each vehicle code digest β'_i on the basis of κ and $\{(\beta'_1, \lambda_1), \ldots, (\beta'_n, \lambda_n)\}$. As a result it generates $\Delta = \{(\beta'_1, \eta_1), \ldots, (\beta'_n, \eta_n)\}$.
  - Sends Δ to LA.
- LA performs the following operations:
  - Each user D can have multiple β_j [2]. For this reason, the LA groups all β_j belonging to the same D and adds their respective η_j. In this way, it obtains the amount that each D has to pay.
  - The amount to be charged to the user's account depends on her contracted rate. For example, users residing inside the LEZ could not pay anything.

SP obtains its benefits from a percentage of the billing and it is therefore not interested in fraudulently reducing the billing amount. Furthermore, as SP knows ξ, it is able to verify the proportional billing amount that it has to receive for each case. Moreover, the user can also obtain the data from her access λ and κ. With this information, the user (mobile application) can verify that the amount to be paid is correct. Supposing

[2] Δ contains the vehicle code digest β'_j but the LA knows the relationship between β'_j and βj.

that one of the parties presents any objection, the collected evidence would be enough to justify the accesses made and the charged fees.

Privacy configuration

SP identifies the system users by means of their vehicles codes digest β_i'. For this reason, any user D can ask for a new code digest β_i^* to the LA in order to prevent that the SP could bind all its accesses. It must be borne in mind that, in a LEZ case scenario, the system does not have data about the users' routes and only the information corresponding to their accesses and exits is available. The change of a vehicle code β_i implies generating new cryptographic keys (Pb^V, Pr^V) and certificate Γ^V for the vehicle. $\beta_{i'}$ is embedded in the common name field. To carry out this process the same operations as in 3.2.2 are performed.

Fraud Control

In the event that any user uses its credentials in a different way than that agreed upon at ξ, for example sharing it among two or more users, it is proposed to use a fraud control unit which would operate in the following way:

- SP performs the following steps:
  - Obtains a symmetric key K;
  - For every registered access χ, its information is recovered from the database. This information includes σ, ρ, δ and the VBD evidence $(\psi, \psi^*, \psi^{''})$. Then, *SP* calculates a new digital signature $\psi^{'''}$ from (ψ, ψ^*) and replaces *D*'s signature $\psi^{''}$ with its own.
  - For each β_i', it generates a list that contains all its accesses $\varrho_i = \{(\sigma_1, \psi_1, \psi_1^*, \psi_1^{'''}), \ldots, (\sigma_m, \psi_m, \psi_m^*, \psi_m^{'''})\}$. In the case the list is empty, the corresponding β_i' is not included.

  - Calculates a masked identity υ_i of β'_i as follows: υ_i=$HMAC_K(\beta'_i)$, where $HMAC_K$ is a secure digest function in combination with a secret cryptographic key.
  - Sends $\Theta = \{(\upsilon_1, \varrho_1), \ldots, (\upsilon_s, \varrho_s)\}$ to the Fraud Control (FC).

- FC carries out the following operations:
  - For each υ_i, validates the information contained in ϱ_i.
    - The signature ψ_i''' of each access contained in ϱ_i is verified. If the verification fails, the access entry is stored for future analysis as its integrity has been compromised.
    - Decrypts the masked identifier ψ^{ID} contained in ψ_i using the FC private key to obtain the VBD identifier ID_i^{VBD}.
    - The VBD proof ψ_i^* of each registered access is checked by means of the symmetric key K^{VBD} of its respective ID^{VBD}. The accesses which fail this verification are considered potential fraud cases and an investigation is conducted.
  - For each potential fraud case detected, the SP is asked to provide the stored VBD access evidence (ψ, ψ^*) signed by D ψ'' in order to prove its honesty.
    - If the signature of D ψ'' is not valid, it is assumed that the SP has compromised the integrity of the data and it is accused of fraud.
    - On the contrary, if the signature is valid and the VBD proof ψ_i^* turns to be invalid, the suspicion falls on D and she is accused of fraud.
  - In a parallel process, FC builds patterns for each υ_i on the basis of the accesses and exits in ϱ_i.

- $*$ Verifies if the entrance and exit registers are feasible in spatial and temporal terms.
- $*$ Verifies if the pattern of accesses and exits of v_i are consistent. For instance, verify if a v_i pattern matches the behavior of a LEZ resident or if a non resident is outside the LEZ at night.
- $*$ If inconsistent patterns are found, the controversial registers are considered potential fraud causes and are stored to conduct an investigation. Revocation of the privacy of v_i is also requested.

3.3 Security and privacy discussion

In this section we discuss the system security requirements. This discussion substantiates the security and privacy properties of the protocol (i.e. the authenticity, non-repudiation and integrity of the exchanged messages, the users privacy, the fairness of the exchange or the fraud avoidance).

The security discussion is organized in five propositions, and each proposition can have several claims to support the fulfillment of the security properties.

The privacy of the proposed system is based on the fact that the different entities do not collaborate with each other to compromise the users' privacy. Privacy is only revoked if exists evidence of an unfair behavior. LA is assumed to be a governmental agency which guarantees the rights of the users, especially their privacy. Without LA cooperation it is not possible to identify a user D. In the payment phase, as the fee amount is aggregated, the LA entity does not obtain enough information to deduce the user's behavior. Moreover, a user can prevent the SP from knowing her access pattern by requesting a new β^*. However, as this process is computationally expensive, a minimum period can be set for a user to request a new β^*.

Proposition 1. *The proposed system preserves authenticity, non-repudiation and integrity.*

Claim 1. *Only authorized users with a registered vehicle can get access to the LEZ*

The access protocol starts with an authentication procedure between the app and the Access Control. This authentication process implies that the user demonstrates the knowledge of the private key from a registered vehicle with respect to its public key certificate (X.509 v3) issued by the LA. In addition to that, the Access Control checks the signature in Γ^V made by LA. So, no counterfeit or forged access tokens will be admitted. Also the user is asked to provide a *binding proof*, which is an evidence that D is using a particular car at the moment when the entrance to the LEZ takes place. The server stores the exchanged messages (χ) since they serve as evidence of the user's access. If the verification of the authenticity fails, then the system takes a photo of the vehicle license plate and the user will be punished. Thus, only users with valid credentials and a registered vehicle bound to her identity can access to the LEZ [3].

In addition to that, the Access Control checks the signature in Γ^V made by LA. So, no counterfeit or forged access tokens will be admitted.

Claim 2. *Users have evidence that they have used the LEZ with the corresponding authorization. The evidence cannot be forged or counterfeited.*

[3] Note that the same verifications are performed at the exit procedure. So, the same security considerations can be applied.

If the access is authorized, AC on behalf of SP sends message $\omega^{'}$ to the user. This token is signed by the AC and has the information related to this action: $\chi : (\sigma, \rho, \delta, \psi, \psi^{*}, \psi^{''}), \beta'$. Therefore, message $\omega^{'}$ is a non-repudiation evidence that SP has allowed a given access. Besides, users cannot counterfeit or forge the proof of entrance $\omega^{'}$ because it is signed by AC using a probably secure signature scheme in order to preserve the authenticity and integrity of the evidence.

Result 1. *From the claims above it can be derived that the system fulfills authenticity, non-repudiation and integrity.*

Proposition 2. . *The protocol avoids the misuse of the access data.*

Claim 3. *The departure proof is linked to the entrance proof. When leaving the LEZ, a driver cannot execute the protocol without the corresponding entrance proof.*

AC verifies that the received access evidence ω and $\omega^{'}$ are valid. This token is signed by the AC and has the information related to this action: $\chi : (\sigma, \rho, \delta, \psi, \psi^{*}, \psi^{''}), \beta'$. Then AC generates a new exit χ' and binds it to the vehicle code digest β'. If a vehicle does not have a valid access evidence, it will not receive the exit data $\omega^{*} = \{\chi', \omega, \omega'\}$ and its digital signature $\omega^{*'}$ as a proof of the vehicle exit to D.

Claim 4. *The entrance proof obtained by a vehicle cannot be used by another vehicle to leave the LEZ.*

During the entrance protocol the AC has stored $\chi : (\sigma, \rho, \delta, \psi, \psi^{*}, \psi^{''}), \beta'$. Now the vehicle leaving the LEZ should register their exit. This protocol begins with a bilateral authentication between AC and the driver. During a vehicle exit D sends the signed proof of her last entrance to LEZ ω and $\omega^{'}$ and AC verifies if the received access evidence ω and $\omega^{'}$ are valid. The the AC generates a new element, χ', binded to the vehicle code digest β', and stores it. Due to the fact that $\omega^{'}$ are signed and ω contains $\psi^{''}$, if a vehicle wants to leave the LEZ using the entrance proof of another vehicle then the the signature $\psi^{''}$ will not correspond with the authenticated driver.

Result 2. *The data provided by the AC to the driver cannot be used fraudulently.*

Proposition 3. *The access system presented here preserves the privacy of the honest users and protects their anonymity, avoiding the traceability of their actions.*

Claim 5. *The system guarantees the anonymity of honest users.*

In order to access the LEZ any user has a Γ^{V}. So, the information about her identity is hidden beneath the code β' inside Γ^{V}. This code is bound to the user's identity. However, only LA knows this relation and only will disclose the identity in case of fraud as it is established in the correspondent protocol. If the vehicle has a consistent pattern of its journeys (i.e. there is a correlation between the in/out journeys identified by the pseudonym), no further actions will be carried out by any entity involved in the protocol so as to identify the user. Thus, if the user follows the protocol, her privacy is respected.

Regarding the payment phase, SP only can know the amount that each β' has to pay on the basis of κ. Only LA can disclose the identity of a user. The payment method used between users and LA in order to pay the fee is beyond the scope of this paper.

Note that, it is assumed that LA is a governmental agency and it will act as a trusted third party. So, LA guarantees the privacy of the honest users either in fraud control or in the payment procedure.

Claim 6. *The access protocol does not allow to trace or to link all the actions of the users.*

SP identifies (by means of β') user's vehicles when they enter (or exit) the LEZ. So, any entry or leaving operation cannot be connected to the user's identity. Besides, any user can prevent the SP from knowing her access pattern by requesting new codes for her vehicles. Since, LA can issue new β^* codes and, in this way, users can unhook her different journeys. Thus, the SP could not bind her accesses even they are made with the same car. So, SP is able to obtain mobility data from the vehicles that enter the LEZ. This can be useful to manage the LEZ but, it cannot disclose the user's identity. Also, it is important to notice that the collected information only concerns the operation of entry or leaving the LEZ, but not the route of the cars inside the zone.

Claim 7. *The system allows the identification of dishonest users.*

On the one hand, the system is not able to identify any user with valid access credentials. On the other hand, the system can identify any dishonest user. The system discloses the identity of users when:

- SP detects an unauthenticated vehicle, and then the system takes a photo of the vehicle license plate.
- FC detects a pattern of a set of related journeys of the same car's code that is not consistent. Note that, SP provides mobility data to FC in order to detect inconsistent patterns.

Consequently, LA will only reveal the user identity if the FC and SP present evidence of an inconsistent pattern of the journeys associated to a code β' or when the sensor takes a photo of an unauthorized vehicle. Otherwise the connection between vehicle's code and its user remains private.

Result 3. *The system preserves the privacy of the users, since her movements cannot be recorded and linked to her identity.*

Proposition 4. *A user cannot act fraudulently, that is, in a way that doesn't follow its contract.*

Claim 8. *Users cannot cheat about its car pollutant category.*

A vehicle binding proof is generated each time D wants to get access the LEZ. The proof is generated by the VBD that is a non-removable device attached to the car. The proof is cryptographically signed (see section 3.2.2) and works as a confirmation that the app used by D is inside the car at the moment she accesses the LEZ. Moreover, the AC verifies whether the emission category of the vehicle of this evidence matches the one included in the certificate of the vehicle Γ^V.

Claim 9. *A non-resident user cannot use the system as a resident.*

During the registration phase the user sends her registration information, which includes the residence certificate in case of being a citizen who is living inside the LEZ area. This information is verified by the LA. However, if a user tries to cheat and uses the certificate of a resident user, the anomalies detection system used by the FC will find an incoherent pattern in υ_i (i.e. a resident that enters the LEZ in the morning and leaves at night). In these cases, the revocation of the privacy is considered to verify that whether the driver is actually a resident or not.

Claim 10. *The system avoids an attack based on multiple identities.*

According to the *Register* protocol, any user D can contact many times with the LA and get some different identities α,s. Also, she can properly install the mobile app many times by using the *Installation of the Mobile Application* procedure specified in section 3.2.2. However, the vehicle registration that binds the user with the vehicle and enables the user to make of the system can only be executed successfully once for each car. Since, the LA checks the vehicle data and it only allows the registration to the owner of the vehicle. Thus, the driver D can just use the application with the vehicle code β that she owns and has received from the LA, no matter how many α,s she has.

Result 4. *As a consequence of these verifications, any driver cannot use the vehicle of another person to take advantage of the better fee scale. Moreover, a user cannot use one of her vehicle certificates with another of her cars without being detected by the system. Also, she cannot get any advantage in registering several times because her identity has to be linked to a vehicle code in order to use the system.*

Proposition 5. *The Driver cannot falsely be accused of not paying her accesses to the LEZ.*

Claim 11. *SP cannot add any fake access to the LEZ from any D.*

In case of fraud the SP has to provide a valid evidence of the D access to the LEZ. However, in order to access a LEZ, D has to send ψ to AC.

This item is a request to access the LEZ and D signs it with the private key associated to the certificate Γ^V (each access request is linked to the pseudonym of each car β' that is inside the certificate). Thus, neither AC nor SP cannot falsely build a fake access of any D because they cannot generate a valid proof of a driver's request to access the LEZ, since only D knows the secret key of a vehicle and only LA knows the relation between D and the vehicle code β.

Claim 12. *SP cannot successfully add journeys of any code digest car β' so as to earn more money.*

At the payment stage (see section 3.2.2) the SP could provide a fake λ_i. However, this fake string of accesses will cause an increase in the bill of the D associated to the car of λ_i. But, as it is noted in section 3.2.2, any user can know the amount of money she should pay and, therefore, if this amount does not match the one requested by the LA, then she can raise a claim and present the evidence of her accesses. As we have stated bellow, neither SP nor AC cannot generate valid proofs of access to the LEZ because they need the signature of the private key associated to each car by the certificate Γ^V.

Result 5. *The system meets the property of exculpability because the SP cannot falsely accuse any honest driver of committing fraud.*

3.4 Experimental Results

This section studies the feasibility of the proposed approach in a realistic scenario (i.e., an scenario consistent with the Technology Readiness Level 5). In particular, the main purpose is to evaluate the parts of the protocol which are subjected to real-time computing (RTC) and whose execution is, therefore, bond to specific time constraints.

3.4.1 Test Scenario

The lifecycle of the protocol defined in this work is divided into the 8 phases specified in Section 3.2.2. Most of these steps are not subjected to RTC and their computational or communication costs have little impact on the feasibility of the implementation; for this reason, their functional analysis is out of the scope of this study. Conversely, the Access (Section 3.2.2) and Exit (Section 3.2.2) steps are bound to strict temporal constraints, since both validation processes should be completed before the vehicle crosses the imaginary line delimiting the restricted area.

In order to evaluate the performance of our system in a real-time scenario, we have implemented the respective prototypes for the entities involved in the Access step of the protocol: Ds and AC. First, a handy stand-alone infrastructure was built to impersonate the AC. This entity was implemented in accordance to the scheme outlined in Section 3.1. On the Ds side, an Android application was written for Ds, capable of interacting with the aforementioned AC infrastructure. It should be noted that the Exit step shares the same actors and processes, so all the experiments and conclusions linked to the Access step are applicable to the Exit step as well. In this way, from now on, we will only mention the Access step for brevity.

With this deployment, two lines of experiments are conducted. The first part of the experiments is performed in the laboratory under a controlled environment in order to study the response of the proposed system under optimal conditions. For this purpose, the AC infrastructure was placed in an interference-free environment with the user's Smartphone in a direct line of sight. It should be noted that the smartphone running the user's application remained static during this test. The results obtained under these settings lead to the definition of a threshold of the minimum conditions for which our system is feasible.

In the second part, outdoor experiments were performed to evaluate the system's behavior on a realistic scenario. For this testbed, a low traffic industrial area was chosen to validate the TRL5 level of technology maturity. The AC infrastructure was placed on a single direction road of the aforementioned industrial area, deploying it as illustrates Figure 3.1 on Section 3.1. On the other side, the user's Smartphone was placed inside a car in the co-driver's seat, remaining untouched during the whole process. Under this setup, the Access step feasibility was validated by repeatedly driving through the AC infrastructure at speeds of 20, 30, 40 and 50 km/h respectively. Through those experiments, the impact of speed and body of the vehicle over the response of our system were expected to be determined.

For both defined phases, we established a confidence interval of 20 tests for each experiment.

3.4.2 Implementation

The testbed configuration and parameters are the following. Each of the three modules that compose the AC is running on an independent Raspberry Pi 2 with a 900MHz quad-core ARM Cortex-A7 CPU, 1GB RAM, Raspbian OS and 5 Vdc battery powered. The Wake Module is equipped with a Bluetooth 4.0 device LM506/Class1 to periodically generate beacons. The Authentication Module is equipped with a Bluetooth 2.1 device LM540 and a 9dBi antenna to communicate with the client's application. Finally, the Virtual Barrier has a presence detector and a monochrome camera built-in to detect and take photos of unauthenticated vehicles. The protocol implementation running in the AC modules was written in Java7 (opendjk-1.7). On the client's side, the Android application was written in Java8 and is running on a LG Nexus 5 with a Qualcomm MSM8974 Snapdragon 800, Adreno 330 GPU, 2GB Ram and Android 6.0 SO.

Communication between AC's infrastructure and Ds' Smartphones is established via Bluetooth. As stated in AC hardware specifications, the Bluetooth version used for communication is 2.1, which is more widespread and grants a greater degree of compatibility with nowadays devices. It should also be noted that, as AC modules are physically separated, they communicate with one another via WiFi through a secure connection.

In this testbed, signatures and encryptions are computed using the RSA cryptosystem with 2048-bit key sizes. Furthermore, during Access and Exit steps, symmetric encryption is used for managing session keys. AES encryption scheme with 256-bit keys is used for this purpose.

3.4.3 Performance Evaluation

Given the testbed specifications defined in the previous section, a series of experiments were conducted in order to evaluate the feasibility of the system proposed in this work.

Laboratory results

The results obtained for each test performed in the laboratory are shown in Table 3.2. According to these results, an average time of 3.502 seconds is needed to complete the whole Access phase, which covers all operations from the awakening the Smartphone application until the completion of the authentication process.

On the basis of the results in Table 3.2, a best case scenario takes 2.583 seconds to complete the Access step under optimal conditions. This time could be considered as the minimum time required by a user to complete the whole process. Therefore, it should be assumed that it is not possible to complete the Access step in a shorter time period. On the contrary, in a worst-case scenario a total time of 4.454 seconds is required. Considering a urban scenario, where the maximum permitted speed is 50km/h, a vehicle

Table 3.2: General laboratory results in seconds

Iteration	Time	Iteration	Time
1	4.365	11	3.205
2	3.310	12	3.356
3	3.694	13	3.321
4	3.000	14	3.948
5	2.583	15	3.700
6	3.937	16	3.403
7	3.985	17	3.769
8	4.454	18	3.850
9	3.816	19	2.668
10	3.136	20	3.540
Average	3.502	Deviation	.502

would travel close to 61.86 meters within that time interval. Therefore, it would be necessary that AC's Bluetooth device range covers at least this distance in order to successfully terminate any access process for the defined scenario. This range has been taken as reference for the deployment of the infrastructure during the field experiments phase.

Another aspect that can be inferred from Table 3.2 is the degree of variability of the tests results, which is reflected in the 0.502 seconds obtained in the standard deviation calculation. In order to unveil the cause of this variation, Table 3.3 broke down the times from Table 3.2 showing the relevant segments of each performed test.

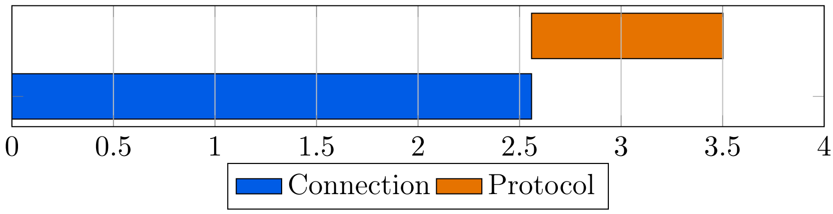


Figure 3.6: Connection time vs. Protocol time in seconds

As previously mentioned, the average time taken to complete the whole

Table 3.3: Laboratory results in seconds

Iteration	Bluetooth	Protocol execution time			
	Connection	Client	Server	Communic.	Total
1	3.321	.098	.313	.633	1.044
2	2.216	.095	.327	.567	.989
3	2.644	.069	.309	.288	.666
4	2.599	.065	.283	.410	.758
5	2.694	.084	.308	.609	1.001
6	2.254	.088	.261	.718	1.067
7	2.286	.102	.281	.331	.714
8	2.838	.091	.302	.717	1.111
9	1.729	.083	.292	.480	.855
10	2.645	.076	.304	.675	1.055
11	3.159	.079	.265	.434	.778
12	2.607	.097	.261	.439	.797
13	2.165	.080	.296	.445	.821
14	2.972	.065	.306	.427	.798
15	3.642	.081	.298	.434	.812
16	3.070	.078	.298	.405	.781
17	2.522	.090	.254	.951	1.295
18	1.560	.080	.292	.737	1.109
19	2.027	.079	.311	.720	1.110
20	2.225	.084	.295	.937	1.316
Avg.	2.559	.083	.293	.568	.944
Dev.	.522	.010	.020	.189	.190
RSD (%)	20.41	12.44	6.75	33.26	20.41

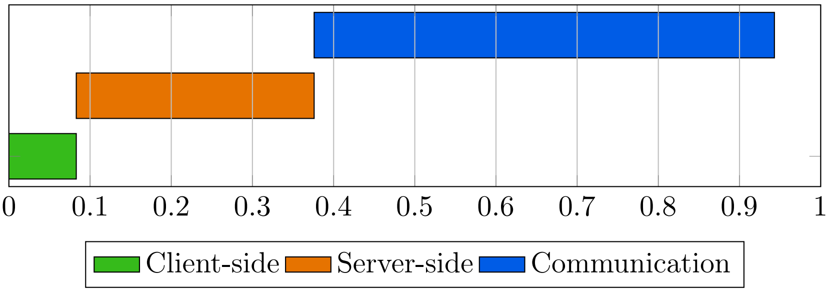


Figure 3.7: Protocol execution time in seconds

Access phase is 3.502 seconds. However, as shown in Table 3.3, this time is not entirely consumed in the execution of the protocol, as Bluetooth connection establishment is also bore in mind when determining the total time of an access process. Figure 3.6 shows the time proportion dedicated to the protocol execution, 0.943 seconds, and to the connection between the client and the server-side Bluetooth devices, which consumes an average of 2.559 seconds. By adding up both times, the aforementioned time of 3.502 seconds to complete an Access phase is obtained.

As it can be inferred from Table 3.3, the average execution time for the Access phase of the protocol takes 0.943 seconds. This same result can be broken down in three stages: client-side protocol, executed on the user's smartphone; server-side protocol, executed by the Authentication Module of the AC infrastructure; and the communication costs. The client-side protocol and the server-side protocol executions take, respectively, 0.083 s and 0.293 s. The difference between the total measured time and the sum of both protocol-sides executions is 0.567 s, which corresponds to communication overheads. These time consumption proportions can be appreciated in Figure 3.7.

The results shown in Table 3.3 clearly show that most of time the Access phase process takes is spent in communication issues. More specifically, the 89.26% of the whole time is dedicated to such tasks: 2.559 seconds to establish connection and 0.568 seconds to transfer the 2,467 bytes that are exchanged during the process. Moreover, the Relative Standard Deviation (RSD) shows that communication and Bluetooth connection are the most unstable times with a variability coefficient of 33.26% and 20.41%, respectively. In non-relative terms, the deviation of Bluetooth connection time, 0.522 s, has a lot more impact in the total phase time than in any other element. Communication cost, with 0.189 s, is the other element which has relevant effect over the degree of variability of Access phase completion time. Either way, it can be concluded that any observed instability in the Access phase completion time is majorly caused due to communication issues. Bluetooth 2.1 technology was chosen to offer a greater support in all kind of mobile devices. In the light of the obtained results, it is considered to investigate newer versions of Bluetooth technology which could mitigate heavy connection and communication costs as a future work.

Finally, it also should be noted that disparity between client and server-side execution times is caused by the reduced computational power of single-board computers. Server-side takes, approximately, 3.5 more times to carry out the cryptographic operations needed to complete the strong bilateral authentication during the Access phase. To support this statement, we run the client and server codes in a single Java application on a PC Intel Core i7-4770S 3.10GHz with, 12 GB and Windows10. Under the same hardware conditions, the protocol execution times are 0.025 s for the client-side and 0.011 s for the server's. These results prove that the operations on the client's side are more computationally costly and the major computation cost on the server-side is due to the use of a low-cost single board computer.

Table 3.4: Field results in seconds

		Bluetooth	Protocol execution time			Total
		Connection	Client	Server	Comm.	
20	Avg.	4.79	.075	.284	.721	5.87
	Dev.	1.23	.012	.017	.231	1.22
30	Avg.	4.65	.077	.285	.678	5.69
	Dev.	.67	.010	.014	.202	.77
40	Avg.	3.36	.074	.291	.632	4.36
	Dev.	.54	.015	.016	.231	.51
50	Avg.	3.24	.089	.286	.660	4.28
	Dev.	.74	.013	.016	.217	.81

Field results

On the basis of the results obtained in the laboratory, the final settings for the field scenario defined in Section 3.1 were shaped. Although the experiment deployment was already set, determining the distances between AC modules required further consideration. On the light of the minimum required Bluetooth range to complete an entire Access step in the laboratory, we placed the Wake module at a distance of 55 meters from the Authentication module. Equally, the distance between the Authentication and the Virtual Barrier module was also of 55 meters. Under this setup, a vehicle disposes a total range of 110 meters to perform all the processes required during the Access step.

Table 3.4 collects the outcomes of the 20 performed tests for different vehicle speeds. The temporal cost of the access phase tests are split up in the same segments as in the laboratory results section: Bluetooth connection, time to establish connection between the client and server-side Bluetooth devices; client-side computation, run time on the user's smartphone; server-side computation, run time on the Authentication Module of the AC infrastructure; and the communication costs.

The obtained results show average times of 5.87, 5.69, 4.36 and 4.28 sec-

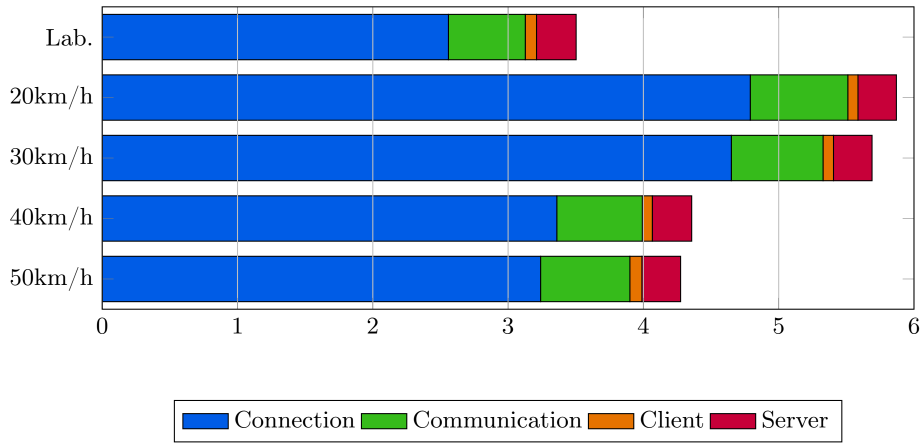


Figure 3.8: Access phase average time completion at different speeds

onds to complete the access phase for 20, 30, 40 and 50 km/h respectively. This represents average increases from 0.77 to 2.37 seconds in relation to laboratory tests on Table 3.2. Figure 3.8 graphically shows these upward time tendencies. As it can be appreciated by comparing Table 3.4 and Table 3.3, those overheads are mainly caused by communication processes, namely Bluetooth connection establishment and their respective communications. Notwithstanding the speed, these two segments present, in general, greater time consumption than the tests performed in the laboratory. Moreover, the client-side and server-side computation show a stable run time in tests performed during laboratory and field experimentation phases alike. This output is expected as protocol's computational cost and devices' computational power are not influenced by the environmental changes of the proposed scenarios. Either way, the observed drop in performance in Bluetooth communication processes can be caused by a combination of several factors bind to the Bluetooth signal power, like the distance between the AC's Authentication Module and the client's device, the speed and the body of the vehicle.

More accurate conclusions can be extracted from Table 3.4 when comparing the access phase completion times at different speeds. The average times of 5.87, 5.69, 4.36 and 4.28 seconds, graphically represented in Figure 3.8, reveal a general decrease of access phase completion times as the speed of the vehicle increases. As previously stated, the variance on the obtained results is almost entirely caused by communication processes. Therefore, Bluetooth connection and communications should be analyzed in order to understand such behavior.

In the same vein, the Bluetooth connection times follow the same tendency and keep decreasing when the authenticating vehicle circulates at higher tested speeds. Table 3.4 shows average times of 4.79, 4.65, 3.36 and 3.24 seconds for 20, 30, 40 and 50 km/h respectively. In order to understand this behavior, it should be borne in mind that the vehicle is gradually approaching the Authentication module which builds-in the Bluetooth device. Considering the Wake module is placed 55 meters away from the Authentication module, the mobile application awakes approximately at this same distance and, therefore, a low signal strength is expected. While the authentication process is running, the vehicle keeps approaching the Authentication module and, consequently, a better Bluetooth signal is received. Against this background, at higher speeds more distance is covered and a greater part of the Bluetooth connection process is done under better signal conditions. For example, two seconds after the mobile app has awakened, the vehicle is 43.8 meters away from the Authentication module if it is traveling at 20 km/h. On the contrary, at speed of 50 km/h the vehicle is much closer at a distance of 22.2 meters.

Regarding the communication costs during the protocol execution, Table 3.4 also shows the average costs of transmitting data between the driver's smartphone and the Authentication module of the AC. These communication costs are 0.721, 0.678, 0.632 and 0.660 seconds for 20, 30, 40 and 50 km/h respectively. Unlike Bluetooth connection establishment, these costs show quite stable times regarding the vehicle speed. Such behavior can also be explained through traveled distance and proximity to the Authentication module. According to the analyzed connection average times, a vehicle approximately travelled 26.6 meters for 20 km/h, 38.75 meters for 30 km/h, 37.3 meters for 40 km/h and 45 meters for 50 km/h when the Bluetooth connection is established and the protocol execution starts. At this point, the distance between the client and server devices is sufficiently close in order to receive stable power signal conditions. A vehicle travelling at 20 km/h is still quite far from the Authentication module, which could explain the slightly higher communication costs.

In summary, it can be concluded that the most restrictive scenario concerns to the experiments made at 50km/h. Even when these test results reflect better completion times, the vehicle ends traveling longer distances due to the fact that it circulates at a greater speed. Considering the 4.28 seconds needed to complete the access authentication process, a vehicle would travel close to 59.44 meters within that time interval, range that can be covered by the Bluetooth LM540/class1 device build-in in the AC's infrastructure. In the light of these experimental results, it can be stated that our system validates the TRL5 level of technological maturity and, therefore, its feasibility in a relevant environment was proved.

Comparative

The results of the conducted experiments in Sections 3.4.3 and 3.4.3 have proved the feasibility of our system in a relevant environment even when low cost AC's infrastructure with reduced computational capabilities is used. Even when our system has proved to be light enough to correctly operate in such conditions, a comparison between the closest schemes in the

Table 3.5: Computation time comparison in seconds

	Client	Server	Total
Our scheme	.083	.293	.376
[16]	1.321	.582	1.903
[17]	1.339	.662	2.001

literature is presented in order to reaffirm its lightweight property. Among the works reviewed in the literature in Section 2, schemes in [9, 10, 11, 12, 13, 14] are not suited for a fair comparative study as they do not implement real-time computing in their phases and they are based on periodical offline verifications of the vehicles' traveled data. Furthermore, this methodology leads to a checkpoint-based fraud detection system, which does not meet the privacy requirements we aimed for. Conversely, the works in [16, 17] are good candidates for evaluating the lightweight property of our scheme, as they present similar privacy features and they also implement RTC entrance and exit phases.

Bearing this in mind, protocols' entrance phase of [16, 17] have been implemented in order to test them against our system. As a fair comparison is desired, the testbed configuration and parameters are the same as the ones defined in Section 3.4.2. Under this scenario, we run 20 tests for each approach to obtain their computational response times. It should be noted that protocols in [16, 17] require that a secure element (SE) generates the digital signatures at the user's side, which, in their works, is simulated by using Smartcards. As this condition cannot be met with an android application, we used the original test results published in those articles for this specific step of the entrance phase.

Table 3.5 shows the average amount of time dedicated to computation tasks, during the entrance phase, by each of the mentioned schemes. Results of [16, 17] were obtained as described above, whilst our approach times were extracted from Table 3.2. As it can be appreciated, our proposed scheme is more lightweight than their counterparts in the literature. The presented results show that lower computation times are achieved both by the server side, run by the AC, and the client side, run by the user's devices, for the same exact conditions. Client computation times of [16, 17] draw special attention as they last more than 1.3 seconds to complete. This is mainly caused by their signature and credentials regeneration strategy through Smartcards, which is the cornerstone of their system's privacy.

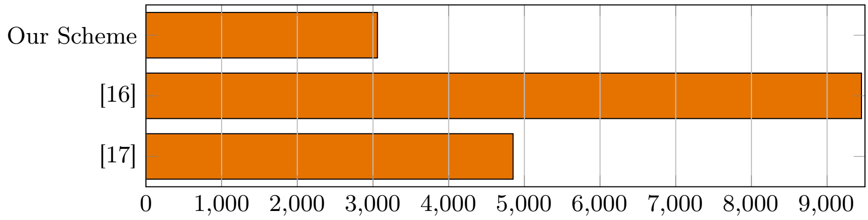


Figure 3.9: Communication costs in bytes

Regarding the communication costs, Figure 3.9 displays the volume of transferred data, in bytes, between the AC and the clients' devices during the entrance phase for each of the aforementioned protocols. As it can be seen, in accordance with the experiment sections in their corresponding articles, protocols on [16] and [17] transmit a total of 9,454 and 4,851 bytes respectively during the entrance phase. In this same stage, our experiments reveal that the proposed system only exchanges 3,059 bytes of data between the AC infrastructure and the client's device. That is, 1,792 and 6,395 less data bytes if it is compared with [17] and [16] respectively. It should be noted that, for our system, the digital certificates are taken into account when calculating the total transmitted bytes, as their sizes may be relevant to determine the communication's overheads. However, in [16, 17] no details are given about how transmitted bytes are calculated, so it is not possible to determine if their measures also include them.

In a nutshell, it can be stated that our system is more lightweight than other similar works in the literature. On the one hand, our system presents lower computational times, for both infrastructure and client sides, when it is executed in the same exact conditions. On the other hand, it also exchanges less data during the interactions between the users and the system's infrastructure, which grants less communications overheads when the same technology is used.

Chapter 4

Privacy-Preserving and Secure Decentralized Access Control for LEZs

According to the centralization issues identified in the literature, in this chapter we propose a new secure and privacy-preserving solution for controlling the access to LEZ*s*, whose fundamental principle is the omission of centralized third parties from taking part in payment related processes in favor of the decentralization that technologies like blockchain and smart contracts [27, 28] provide.

In our approach, through the use of smart contracts, interactions between users and LEZ's infrastructures are processed as blockchain transactions, thereby permitting the corresponding fee to be automatically calculated and charged from the user's wallet in terms of digital tokens. Under this procedure, entities responsible for registering vehicle accesses and charging their corresponding fees are replaced by a decentralized network, which grants the verifiability, reliability and transparency of the uploaded events. Therefore, there is no need for entities to locally store signed proofs of every interaction they made, as any node belonging to the distributed network can verify the validity of the transaction flow in the blockchain. Taking this approach, however, has no impact on the privacy of honest users and preserves the revocable anonymity property like other works in the literature do. This proposal is supported by a publication in [29].

The remainder of this chapter is organized as follows. Section 4.1 introduces the blockchain and smart contract technologies in which our system relies on. Section 4.2 introduces the new proposal and its novelty. Section 4.3 details the protocols that sustain the proposed system. Finally, Section 4.4 analyzes how the new proposal fulfills the security and privacy requirements considered in our scenario.

4.1 Background

In this Section we provide the background on Smart Contracts technology and the underneath Blockchain paradigm on which they are implemented.

The blockchain paradigm, originally designed for financial accounting [27], was extended in [28] to a generalized framework permitting two entities to decentrally settle transactions of arbitrary resources without the involvement of a trusted third party. Ethereum[1] was the first attempt to implement this idea, whereby programmable logic programs, referred to as smart contracts, are executed on a turing-complete virtual machine and their computing results are stored in a public blockchain once the network nodes have reached a state consensus.

[1] Ethereum Project, https://www.ethereum.org/

4.1.1 Blockchain

The advent of Bitcoin in 2009 by Satoshi Nakamoto [27] is considered as a turning point in the evolution of digital currency. The creation of Bitcoin was revolutionary not only for being the first decentralized crypto currency but also for bringing mainstream concepts like blockchain and smart contracts.

The first work based on a cryptographically secured chain of blocks [30] was first presented in 1991 by Stuart Haber and W. Scott Stornetta, who wanted to implement a system where document timestamps could not be tampered with. This concept was continuously improved throughout that decade until the first blockchain was conceptualized by Satoshi Nakamoto in 2008. The design proposed by Nakamoto, using a Hashcash-like method to add blocks to the chain without requiring them to be signed by a trusted party, was later implemented as a core component of Bitcoin cryptocurrency, where the blockchain serves as the public ledger for all transactions on the network.

A blockchain is a digitized, decentralized, distributed database, commonly referred to as a distributed ledger that records all the transactions introduced in the blockchain network across many computers in a way that any involved record cannot be altered retroactively. The blockchain database can be seen as an ordered list of blocks, where each block is identified by its cryptographic hash and arranged in a way that it references the block that came before it, leading to the creation of a chain of blocks. The database is replicated and shared among the network participants, allowing them to verify and audit transactions independently and relatively inexpensively. The management of blockchain databases is performed autonomously using a peer-to-peer network and a distributed timestamping server, in which transactions are validated by mass collaboration of nodes motivated by collective self-interests.

Blocks

A block of the blockchain can be defined as batches of valid transactions that are hashed and encoded into a Merkle tree [31]. Each block also contains the cryptographic hash of the previous block, linking both of them and forming a chain. This chain forms an iterative process confirming the integrity of the preceding block, all the way back to the original genesis block.

Each block contains, among other things, the current time, a non-empty list of recent transactions, and a reference to the preceding block. It also contains an answer to a difficult-to-solve mathematical problem, known as proof-of-work, whose answer is unique to each block. In order to submit a block to the network, it is mandatory to known the correct answer to this mathematical problem. The process of nodes competing to be the next to find the answer to that problem and solving a block is what it is known as "mining". Although the mathematical problem of a block is extremely difficult to solve, once the answer is found, it is very easy for the nodes of the network to confirm that the solution is correct. There are multiple valid solutions for any given block, but only one solution needs to be found for solving the block.

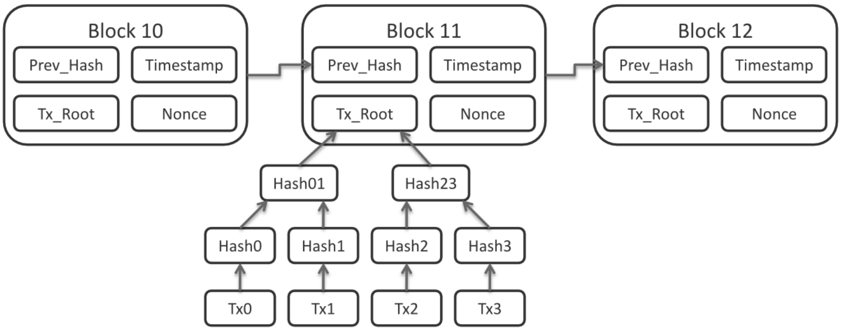


Figure 4.1: Graphic of data fields in Bitcoin block chain

When a new block is created and appended to the blockchain, all the information contained on it will be available to every member of the network. One important aspect is that once the information is introduced into the blockchain, it is very difficult to modify it because it requires the consensus of all the participants involved. The average time that it takes the network to generate one new block in the blockchain is known as block time and it defines how fast the transactions are validated. The block time for Ethereum is taking between 14 and 15 seconds, while for Bitcoin takes around 10 minutes.

Decentralization

Every node in the peer-to-peer network stores a copy of the blockchain, whose data quality is achieved through massive database replication and computational trust. In this way, there is not an "official" centralized copy of the blockchain as all nodes in the network are trusted the same regarding the copy they are holding. The advancement of the blockchain is produced when client nodes broadcast their transactions to the network. Mining nodes validate these transactions, add them to the block they are building, and then broadcast the completed block to the other nodes. Then, the nodes reach consensus for defining the next valid block in the blockchain through the use of a distributed consensus algorithm like prof of stake, which involves the solving of computationally intensive puzzles.

By following this approach, the blockchain stores data across its peer-to-peer network, eliminating the risks associated with data being held centrally and avoiding a central point of failure. Blockchain security also includes the use of public-key cryptography. The public key acts as an address in the blockchain. Conversely, the private key serves as a password, giving its owner access to their digital assets and the means for interacting with the capabilities that the blockchain supports.

4.1.2 Smart Contracts

The first definition of a smart contract was first coined in 1994 by the computer scientist and cryptographer Nick Szabo, who define it as: “A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises”.

Nowadays, a smart contract is a piece of executable code that runs on top of the blockchain which facilitates, executes and enforces an agreement between untrusted entities of arbitrary resources, without the need of a trusted third party. Contrary to a traditional contract which clearly defines the rules and penalties subject to an agreement, a smart contract automatically enforces the obligations of the parties involved, which, in the end, significantly reduces the transaction costs which in turn facilitate more advantageous trades.

As smart contracts are built on top of the blockchain technology, they require a blockchain platform in order to be developed and deployed. Bitcoin [27], limited to the currency use case, and Ethereum [28], currently the most common platform for developing smart contracts, are the most widespread blockchain public platforms. Ethereum provides a blockchain with a built-in Turing-complete programming language, allowing anyone to write smart contracts and decentralized applications where they can create their own arbitrary rules for ownership, transaction formats and state transition functions. Following this principle, Ethereum’s smart contracts provide a large set of functionalities:

- Function as “multi-signature” accounts, so that funds are spent only when a required percentage of people agree.
- Manage agreements between users.
- Provide utility to other contracts.

- Store information about an application, such as domain registration information or membership records.

4.2 Our proposal

As previously introduced in Chapter 2, current LEZ access control systems in the literature rely on centralized trusted entities to keep count of the circulation fees that a vehicle's owner has to pay at the end of a billing period, introducing a single point of failure in the system and, therefore, endangering its security and availability.

Our scheme introduces a new privacy-preserving approach where third parties are omitted from payment related processes in favor of decentralization that blockchain technology offers. Under this premise, every access to the LEZ is considered as a transaction and, through smart contract interaction, published into the blockchain. In the same way, according to the transaction's uploaded access parameters, the smart contract automatically charges the corresponding fee amount in terms of digital tokens.

4.2.1 Entities

Our system involves the following actors: i) LEZ Administration (LA); ii) Drivers (D); iii) Access Control Infrastructure (AC); and iv) Cryptocurrency Mixing Service (M).

The LA is the entity in charge of managing the LEZ. Among its tasks, it is responsible for fixing the access rules, the price and deploying the smart contract which manages the accesses and payments of the system. Drivers (D) are the group of users whom the approach is addressed to. Ds's vehicles should be equipped with an on-board unit (OBU), which is expected to be a tamper-proof device with cryptographic capabilities and equipped with GPS technology, 4G communications and short range communications (e.g. Bluetooth). The AC*s* are infrastructures that control the D*s* accesses to the LEZ. These infrastructures may be under control of one or more for-profit entities as long as the LA is not one of them. Finally, *M*) it is an independent entity responsible for anonymizing cryptocurrency transactions, in exchange for a fee, during digital wallet renewal process, so that transferred funds cannot be trailed back to the original source.

4.2.2 Our proposal in a nutshell

Figure 4.2 shows a general view of the proposed scheme along with the entities involved in the process: the vehicle's OBU, the Access Control infrastructure (AC) and the blockchain network. On this scenario, in order to interact with the AC, it is required that the vehicle's OBU obtains, from the LA, valid credentials which certify its vehicle emissions category and generates a digital wallet in order to pay, through the use of smart contracts, its accesses to the LEZ.

Our protocol starts when a vehicle is entering the LEZ and its OBU automatically awakes without the intervention of the driver, through the detection of *Bluetooth Low Energy* beacons. Given that awakening signal, the OBU establishes a secure connection via short-range wireless communication system with the AC and, through the cryptographic protocol, proves that the user is driving a valid registered vehicle. When the process ends, the OBU and the AC agreed an access receipt which contain the access details and a code to identify the transaction in the blockchain. During the whole process, the user's anonymity is preserved through the use of pseudonyms, which can be changed at will to prevent other entities from binding all her accesses. Conversely, if the authentication process does not ends correctly or is somewhat skipped due to driver's misbehavior, the AC will take a photo of the vehicle's license plate, revoking the privacy of the misbehaving driver.

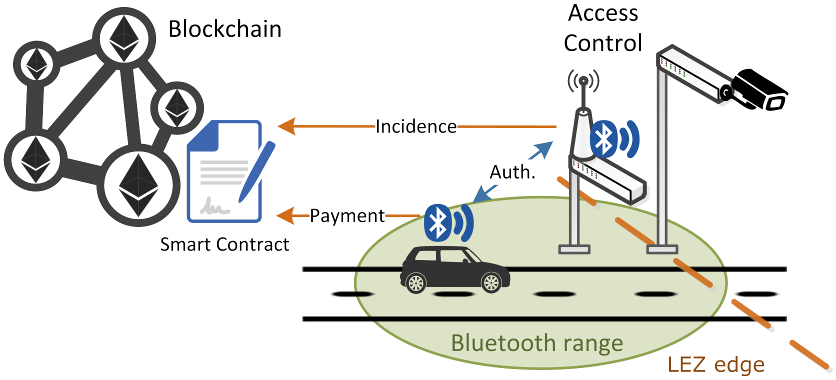


Figure 4.2: General overview of the system

Once the authentication with the AC concludes, the vehicle's OBU interacts with the smart contract, broadcasting a transaction which contain the access receipt with the agreed access parameters. On the basis of these parameters, the smart contract verifies their validity, calculates the amount to pay according to the last uploaded prices list in the blockchain, and charges the corresponding amount in terms of digital tokens, i.e. elements acting as native currency in our system, to the user. Later, when the transaction has been validated and added to the blockchain, the AC involved in the process verifies whether the access transaction has been correctly conducted. If any irregularity is detected, the AC interacts with the smart contract to publish an access incidence in the blokchain, using its own copy of the access receipt to revoke the user's privacy.

4.2.3 Blockchain integration

The new proposal adopts the Ethereum's smart contract technology to endow individual nodes in the blockchain network with the ability to verify the access of vehicles to the LEZ and charge its corresponding fees, without requiring a centralized third party that oversees the whole process. For this purpose, it uses a smart contract whose logic allows the transactions in the system to include access data and digitally signed proofs generated by ACs, which allows network nodes to validate the correctness of those accesses. These operations also involve cryptocurrency transactions, as the smart contract logic also determines the tokens amount to transfer on the basis of date, time and vehicle's emissions category contained in the access data.

According to the blockchain paradigm, an incentive is required for nodes to participate in the network and contribute with their computational resources to validate transactions and achieve trustworthy advancement of the chain. On this matter, the proposed system predisposes some of the envisaged entities as potential encouraged miners: on the one hand, LA is thus incentivized to participate in transaction mining as it is the main provider of tokens that users consume when pay a LEZ access. On the other hand, the ACs, and the organizations supporting them, receive tokens from users as payment for controlling the access of vehicles. As they later receive monetary compensation from the LA according to the total gathered tokens, this evinces the economical motivation that encourages ACs to actively contribute into validating transactions.

4.2.4 Security and privacy requirements

The envisaged attacker model considers both internal and external adversaries. Internal attackers can be any vehicle and any *honest but curious* AC. External entities are those individuals that do not follow the proposed protocols. In any case, adversaries' computational power do not permit them to break current computationally secure cryptosystems. Finally, the LA is considered to be fully trusted.

Against this adversary model, our LEZ access control system is expected to fulfill the following properties:

- *Revocable anonymity for dishonest users.* Users' privacy is granted as long as they follow the proposed protocol. Otherwise the system is able to expose the dishonest user's identity, even if she does not hold any credential.

- *User accesses are non-traceable.* The system provides mechanisms to avoid tracing or linking the user's actions, even when they are published in the blockchain.

- *Non-repudiation and integrity.* The evidences generated from the interaction between entities cannot be denied, forged or counterfeited.

- *Fraud avoidance (exculpability).* A user cannot be falsely accused of not paying her corresponding fees.

4.3 Protocol

This section formalizes the different protocols that drive the proposed system giving enough detail to allow their implementation. These are: *On-board unit set-up*, *Wallet filling, Access*, *Payment* and *Pseudonym renewal.*

4.3.1 On-board unit set-up

The first step consists in configuring the OBU of a user D to obtain the credentials to interact with the system. To this end, the OBU establishes a secure communication channel, via TLS, with the LA servers and provides D's vehicle information (plate number, car maker, model, etc.). It is assumed the OBU cannot be tampered with to provide false information. It is also assumed that the LA belongs to a governmental entity and it is able to obtain the vehicle's owner data from the provided information. When the LA receives the vehicle's data, through a secure channel, it performs the following operations:

- Checks whether the received vehicle's data matches the plate number and obtains the owner's data (name, residence, etc.).
- If the verifications are correct it does the following steps: i) generates a pseudo-random 128-bit vehicle code β; ii) binds the vehicle code β to the vehicle's owner D and; iii) sends β to D through the secure channel.

Once D has received β, continues the process:

- Generates a key pair (Sk^D, Pk^D).
- Generates a certificate request γ^D from (Sk^D, Pk^D). Field *CommonName* contains the previously calculated β, instead of user's personal data.
- Sends β and γ^D to LA.

The LA performs the following operations on the received data:

- Checks the following points: i) β code is in its database and is valid; ii) the *CommonName* field equals to the β; and iii) the certificate request γ^D is valid.
- If previous verifications are not met, the vehicle registration is aborted. Otherwise the process continues.
- Issues the certificate Γ^D. Vehicle emissions category τ is included in the certificate as an extension (X509 v3). The LA may include other extensions (e.g., a LEZ residence proof).
- Sends the generated certificate Γ^D to D.

Finally, in order to complete the registration process, D carries out the following operations:

- Verifies the validity of the certificate Γ^D through Γ^{LA}.
- If the previous verification is correct, Γ^D and (Sk^D, Pk^D) are securely stored.

Once the registration process is completed, as the users have to interact with smart contracts and process payments, D generates an Ethereum digital wallet following the next steps:

- Generates a private key Sk of 256-bit, a public key Pk of 512-bit and derives its address according to Ethereum key specs.
- Securely stores the digital wallet $W(Sk, Pk)$.

4.3.2 Wallet filling

In order to pay their circulation fees through the use of smart contracts, D purchases LEZ tokens from the LA, which will host an Internet portal for this specific purpose. Payment via tokens is expected to be anonymous but the use of classic payment mechanisms (e.g. credit card) to acquire those tokens is a privacy issue that could lead to link all user's accesses. In order to tackle this problem, the next steps are followed each time D purchases tokens:

- Creates a temporal wallet $W(Sk, Pk)_T$ by generating its private key, public key and corresponding address.
- Accesses the payment portal and buy LEZ tokens, which will be transferred to the temporal wallet $W(Sk, Pk)_T$.

- Sends a petition to a cryptocurrency mixing service (M) (e.g., ETH-Mixer[2]) for transferring the purchased LEZ token from $W(Sk, Pk)_T$ to D's digital wallet $W(Sk, Pk)$. M performs the mixing process that obscures the link between $W(Sk, Pk)_T$ and $W(Sk, Pk)$ preventing the selling entity from linking the actual D's wallet with the temporal one.

- Disposes $W(Sk, Pk)_T$ once the tokens have been transferred from it.

4.3.3 Access

This protocol phase begins the moment D enters the AC communication range and both entities establish secure communication, which comprises strong bilateral authentication. Then, the OBU of D carries out the following operations:

- Generates a random 128-bit access ID δ to identify the transaction in the blockchain.

- Generates the access information tuple ψ={δ, position, date, time, τ}

- Generates the digital signature $\psi_D^{'}$ from ψ

- Sends ψ and its signature $\psi_D^{'}$ to AC

On receipt of the access request, the next operations are performed by the AC:

- Verifies that Γ^D certificate is valid and has not expired.

[2] ETH-Mixer, https://eth-mixer.com/

- Verifies $\psi_D^{'}$ signature and checks if the received data contained in ψ is correct. The vehicle category τ is included in Γ^D.

- Checks the presence sensor and verifies whether the detected vehicle has been authenticated. If some verification is not correct, the system takes a photo of the vehicle's license plate.

- If previous verifications are correct, D can proceed into the LEZ. In that case, AC prepares an access receipt $\rho = \{\delta$, position, date, time, $\tau\}$ and its signature ρ'_{AC}, which is signed using AC's digital wallet private key so it can be verified on-chain by the smart contract.

- Sends the access data $\omega = \{\beta, \rho, \rho'_{AC}, \psi_D^{'}\}$ and its digital signature $\omega_{AC}^{'}$ as a proof of D's access.

- Locally stores ω and D's received signature $\psi_D^{'}$ until the fee payment for the registered access is verified.

Finally, D verifies the result of the access ω and $\omega_{AC}^{'}$ along with the data contained in it. The proof of access is locally stored until the payment process is completed.

4.3.4 Payment

The payment phase is based on smart contracts, which manage the fee calculation process without the intervention of centralized entities like a SP or a LA. Namely, D*s*, through smart contract interaction, pay their corresponding access fee, whose transaction consummation, once validated in the blockchain, is verified by the involved AC*s*.

First of all, as an individual step, the LA, which is assumed to be the smart contract's owner, can update the prices used by the smart contract to calculate the access fees. To do so, the LA interacts with the smart contract using the method *set_ prices* which uploads new prices to the blockchain.

Once D completes the access phase and obtains the access receipt ρ, contained in the received data ω, she starts the payment process by interacting with the smart contract remotely calling the method *register_ access*, and uploading as parameters the access receipt ρ and its signature ρ'_{AC}.

Through the call of *register_ access* method, the following operations are processed on-chain:

- Checks whether access δ is already registered in the blockchain and its current status. In case it is registered and its status is set to "paid" no further action is taken. Otherwise the access registration process continues.
- The signature ρ'_{AC} is verified and the address of the signer, which should belong to a registered AC, is disclosed. If any of these verifications are not correct, the state of access δ is updated to "invalid signature".
- On the basis of date, time and τ contained in ρ, the access fee is calculated according to the last registered prices in the smart contract, and the corresponding fee amount is automatically transferred in terms of digital tokens from D to AC. In case D does not have enough funds, the state of access δ is updated to "no funds".
- Access δ is stored and its state is set as "paid". Regardless *register_ access* execution result, the transaction is added to the blockchain.

After a certain period of time, when the access transaction performed by D has been validated and added to the blockchain, the AC involved in the vehicle's access verifies the payment status:

- Gets the current access's state by calling the *get_ access_ status* method through access ID δ.

- Checks if an access with a δ ID exists and it its current status is set as "paid".

- If any of the previous conditions are not met, the involved AC publishes an incidence using the method *payment_ incidence* of the smart contract. With this process, the user's pseudonym β, the access data ψ and D's signature ψ'_D are published in the blockchain. This method takes date and time in ψ as reference to determine if enough time has elapsed to publish an incidence.

- Deletes the local copy of data access ω as it is no longer needed, either because the payment is complete or because the access information has been published in the blockchain for revision.

By following this process, the AC*s* pool LEZ tokens from the correctly validated D*s*' access they register. At some point, the LA, who owns the smart contract, will monetarily reward the AC*s*, or the entities behind them, accordingly to the total amount of LEZ tokens they gathered. Regarding the published incidences, the LA can initiate sanctioning measures against any D holding one. This is possible as D's pseudonym β is included in the incidence data uploaded in the blockchain along with D's signature, which can only be verified with D's certificate γ^D.

4.3.5 Pseudonym renewal

The entities in the system identify users by means of their code β and their blockchain address. For this reason, any D can ask for a new β^* to prevent other entities from binding all her accesses. Changing β implies generating new keys (Sk^D, Pk^D) and certificate Γ^D, as β is embedded in the certificate. In the same vein, D generates a new Ethereum wallet $W(Sk, Pk)^*$ to get a new address when publishing to the blockchain. To carry out this renewal, the same operations as in 4.3.1 are performed.

Once the new wallet $W(Sk, Pk)^*$ is generated, a way to anonymously transfer funds between $W(Sk, Pk)$ and $W(Sk, Pk)^*$ is required. For this purpose, D sends a petition to the mixing service M to transfer remaining LEZ tokens from the old wallet $W(Sk, Pk)$ to the new one, obscuring the trail of transactions between the source and destination wallets.

4.4 Security and privacy analysis

This section explains how the proposed scheme fulfills the security requirements introduced in Section 4.2.4 for the defined adversary model.

4.4.1 Revocable anonymity for dishonest users

In order to access the LEZ, D authenticates herself by means of her public key certificate which do not reveal D's identity since it only contains her pseudonym β. This pseudonym is bound to D's identity, but this relation is only known by LA, which will only disclose it in case of fraud.

In the payment phase, access transactions are published in the blockchain under Ds' address, which act as a pseudonym in this scenario. This transaction does not contain β and, hence, the LA cannot link D's address to her identity.

Conversely, the system can identify dishonest users as, in case of some incident, AC publishes its own access receipt to the blockchain. Since AC's access receipt is signed by D, β is disclosed and LA can take measures against her. In case AC detects an unauthenticated vehicle, the system takes a photo of the vehicle's license plate, disclosing the user identity.

4.4.2 User accesses are non-traceable

AC identifies Ds by means of their β every time they access the LEZ. In order to prevent AC from linking every Ds' access, any D can request to the LA the issuance of a new $\beta*$. In this way, a new key pair and its corresponding certificate are generated, severing all connections with her old pseudonym.

In the same vein, D can generate at any moment a new digital wallet by creating a new key pair and, therefore, a new address, unhooking any involvement with her previous transactions published in the blockchain. In case that funds need to be transferred between wallets, D transfers the tokens through a mixing service which obscure the trail of transactions between source an destination wallets.

During the wallet filling phase, D first transfer the bought tokens to a temporal wallet from where will be transferred, through the mixing service, to the real one. This way, the selling entity is unable to bind the payment information with D's real wallet.

Finally, it is also important to note that collected data in the blockchain only concerns the entrances to the LEZ, but not the route of the vehicles inside the zone.

4.4.3 Non-repudiation and integrity

During the access phase, an authentication process between D and the AC is performed, in which both entities demonstrate they hold a Sk result from the registration process with the LA, through a public key certificate issued by this same entity. As the signature of both certificates is verified, no counterfeit credentials are accepted. At the end of the authentication process, both AC and D receive an access receipt, containing the access data, signed by the counterparty; therefore, it cannot be tampered with.

At the payment phase, D cannot upload forged accesses into the blockchain through the smart contract, as the access receipt contains a signature issued with the AC's digital wallet, which can be verified on-chain. The authorized AC*s*' information and wallet address are public and published in the blockchain by the LA, hence, the signature issuer can be verified.

4.4.4 Fraud avoidance (exculpability)

In case of fraud, the involved AC has to publish an access receipt signed by D to the blockchain. On that matter, it is not possible for any attacker to falsely accuse D, as the only way to obtain such evidence is to complete the access phase which comprises a strong bilateral authentication between both entities.

Chapter 5

Decentralized Privacy-Preserving Access Control for LEZ

In our first and second contributions, Chapter 3 and Chapter 4 respectively, besides tackling the deployability and centralization problems identified in the literature, we focused in designing efficient and lightweight approaches, relying on pseudonyms and periodical credentials renewal in order to preserve the users' privacy. This way of proceeding meets lower computational requirements, but places the system's privacy strength on the users' credential renewal policy and, hence, on their own judgement.

In Chapter 5 we contribute with an efficient privacy-preserving access control system for LEZs, in which the cornerstone is to pursue the decentralization the blockchain paradigm poses, while providing, through a tailored group signature scheme, the users' privacy requirements that the use of a public ledger requires. Unlike other approaches in the literature, our system truly preserves the anonymity, non-traceability and unlikablility of honest users, without the need of a client-on-demand credential renewal process to achieve it. On top of that, experimental results show that our approach is more lightweight than similar group-signature-based LEZ access control systems, although entailing a performance setback regarding our previous contributions. This contribution is supported by a publication in [32].

The remainder of this Chapter is organized as follows. First, in Section 5.1, the cryptographic background of the group signature scheme used in our model is provided. Section 5.2 introduces the new proposal. Section 5.3 thoroughly details the protocol steps of the introduced model. Section 5.4 analyzes the security and privacy requirements. Finally, Section 5.5 presents the evaluation of the proposed scheme and compares it with other literature works.

5.1 Background

In this chapter, a group signature scheme is integrated to the proposed model allowing the system's users to anonymously sign messages on behalf of the group and, therefore, permitting the receiver of these signatures to verify their validity without disclosing sender's identity.

The integrated group signature scheme is presented in [33] and its based on Weak Boneh-Boyen (wBB) signature [34] and the efficient proofs of knowledge in [35]. This scheme has fast signature generation and provides all privacy-enhancing signature features that our proposal requires, i.e. anonymity, unlinkability and untraceability. The basis of this scheme are presented hereunder.

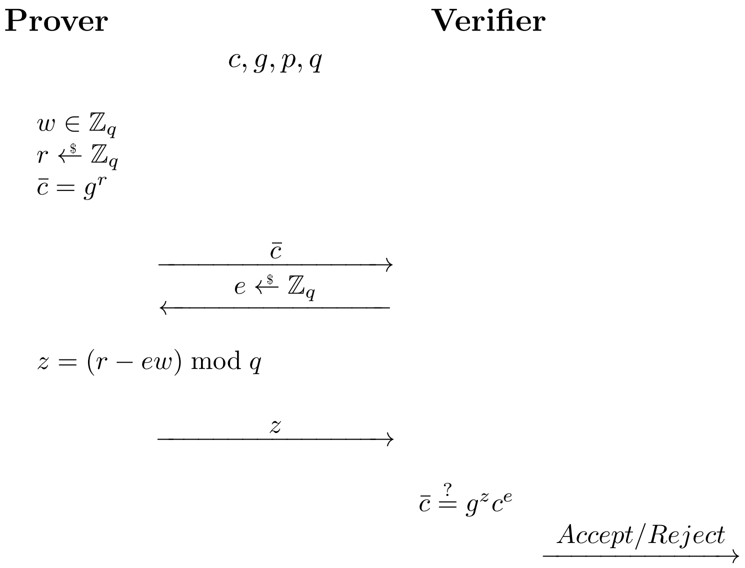

Prover
Verifier
c, g, p, q
$w \in \mathbb{Z}_q$
$r \xleftarrow{\$} \mathbb{Z}_q$
$\bar{c} = g^r$
$\xrightarrow{\bar{c}}$
$\xleftarrow{e \xleftarrow{\$} \mathbb{Z}_q}$
$z = (r - ew) \bmod q$
$\xrightarrow{z}$
$\bar{c} \overset{?}{=} g^z c^e$
$\xrightarrow{Accept/Reject}$

Figure 5.1: Schnorr's proof of knowledge of discrete logarithm

5.1.1 Proofs of Knowledge

Proofs of Knowledge is a protocol for proving the discrete logarithm knowledge based on the the Schnorr signature scheme [36]. Through this procedure, as shown in Figure 5.1, prover proves his knowledge of a discrete logarithm with respect to public parameters c, g, p, q, i.e., he proves the knowledge of $w : c = g^w \bmod p$, where p is prime modulus, q is group order and g is $\mathbb{Z}_p^*$ generator.

The proof of knowledge of discrete logarithms is a 3-way protocol where the prover commits to a random number r in the first step, receives a challenge e in the second step and responds by z to the challenge in the third one. This protocol can be modified to behave as a proof of knowledge signature (SPK) scheme by simply computing the challenge e as $e = \mathcal{H}(e, m)$.

5.1.2 Bilinear pairings

Given cyclic multiplicative groups $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$ of prime order q, with generators $g_1 \in \mathbb{G}_1$ G1 and $g_2 \in \mathbb{G}_2$, a bilinear map is a function $\mathbf{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ with the following properties:

- Bilinearity: $\mathbf{e}(g_1^x, g_2^y) = \mathbf{e}(g_1, g_2)^{xy}$ for all $x, y \in \mathbb{Z}_q$.
- Non-degeneracy: for all generators $g_1 \in \mathbb{G}_1$ and $g_2 \in \mathbb{G}_2$, $\mathbf{e}(g_1, g_2)$ generates $\mathbb{G}_T$.
- Efficient computability: exists an efficient algorithm $\mathcal{G}(1^k)$ that outputs the bilinear group $(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathbf{e}, g_1, g_2)$.

5.1.3 Weak Boneh-Boyen Signature

The weak Boneh-Boyen (wBB) signature scheme [34] can be used to efficiently sign blocks of messages. The signature cannot be randomized, but it can be easily integrated with zero-knowledge proofs, as the efficient proofs-of-knowledge presented in [35], so that the knowledge of signed messages, and signatures themselves, can be proven anonymously, unlinkably and untraceably.

`Setup`: On input security parameter k, generate a bilinear group $(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathbf{e}, g_1, g_2) \leftarrow \mathcal{G}(1^k)$. Take $sk \xleftarrow{\$} \mathbb{Z}_q$, compute $pk = g_2^{sk}$, and output sk as private key and $pk = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, \mathbf{e}, pk)$ as public key.

`Sign`: On input message $m \in \mathbb{Z}_q$ and secret key sk, output $\sigma = g_1^{\frac{1}{sk+m}}$.

`Verify`: On input the signature σ, message m, and public key pk, output 1 iff $\mathbf{e}(\sigma, pk) \cdot \mathbf{e}(\sigma^m, g_2) = \mathbf{e}(g_1, g_2)$ holds.

5.1.4 Group Signatures from Randomizable Proofs of Signatures

Group signature [22] allows the sender to anonymously sign a message on behalf of the group and, therefore, a receiver to verify that it is a valid signature without disclosing sender's identity. In other words, this approach provides data authenticity without disclosing the users' identity. Moreover, it is possible to revoke malicious users, i.e. the signature can be "opened" in case of fraud.

The group signature scheme we integrated in our LEZ scheme was presented in [33]. This work propose a novel group signature scheme based on wBB signatures [34] and the efficient proofs-of-knowledge in [35]. This scheme has fast signature generation and provides all privacy-enhancing signature features, i.e. anonymity, unlinkability and untraceability. The following cryptographic algorithms and protocols define this group signature scheme:

$(pk, sk_m, par) \leftarrow$ `Setup` $\leftarrow 1^{\mathcal{K}}$: the algorithm inputs the security parameter $\mathcal{K}$ and generates the bilinear group along with the public system parameters $par = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathbf{e}, g \in \mathbb{G}_1, g_2 \in \mathbb{G}_2)$ satisfying $|q| = \mathcal{K}$. It also generates the manager's private key $sk_m \xleftarrow{\$} \mathbb{Z}_q$ and computes the public key shared by all users $pk = g_2^{sk_m}$. It outputs the (pk, par) as a public output and the sk_m as the manager's private output.

$(sk_i, rd) \leftarrow$ `Register` $\leftarrow (id_i, sk_m)$: On the input of the manager's private key sk_m and the user's private identifier id_i, the protocol outputs the user's private key $sk_i = g^{\frac{1}{sk_m + id_i}}$ and updates the manager's revocation database rd by storing id_i.

$sig(sk_i, m) \leftarrow$ `Sign` $\leftarrow (m, id_i, sk_i)$: on the input of the user's identifier id_i, his private key sk_i and the message to sign m, the algorithm outputs the signature $sig(sk_i, m)$ consisting of $(g', sk_i', s\bar{k}_i, \pi)$. Where g' is the generator g^r raised to a randomly chosen randomizer $r \xleftarrow{\$} \mathbb{Z}_q$; sk_i' is the users's private key raised to the randomizer sk_i^r; $\bar{sk}_i$ is the randomized private key raised to the user identifier $sk_i'^{-id_i}$; and π is $SPK\{(id_i, r) : \bar{sk}_i = sk_i'^{-id_i} \wedge g' = g^r\}(m)$, i.e. the proof of knowledge of r and id_i signing the message m.

$0/1 \leftarrow$ `Verify` $\leftarrow (sig(sk_i, m), m, pk)$: the algorithm inputs the message m, its signature $(sig(sk_i, m)$ and the public key pk. It checks the proof of knowledge signature π and checks that the signature is valid with respect to the manager's public key using the equation $\mathbf{e}(\bar{sk}_i g', g_2) \stackrel{?}{=} \mathbf{e}(sk_i', pk)$.

The algorithms and protocols of this scheme fulfill the security properties hereafter, as long as the manager is trusted not to impersonate the entities issuing signatures.

- *Correctness*: signatures are verified correctly if generated by valid and honest users.
- *Anonymity*: all signatures are anonymous, untraceable and unlinkable to all entities except the manager.
- *Traceability*: the manager can de-anonymize, link and trace signatures.

5.2 Model of the system

As stated in Chapter 2, similar works in the literature provide privacy to their users by means of pseudonyms or group signature schemes, which require periodical credential renewal processes to continue providing anonymity, non-traceability and unlikablility. Namely, the privacy-preserving strength of these schemes mostly rely on their pseudonym renewal policy, whose regeneration process in the end falls on the client-side and, hence, on the users' criteria.

The presented scheme introduces a novel decentralized privacy-preserving access control system for LEZs based on group signatures which provides anonymity, non-traceability and non-linkability to honest users without the need for credentials regeneration to preserve it. Last but not least, it continues the decentralized trend presented in Chapter 4 which allows the decentralization of vehicle access acknowledgements and their corresponding payments by means of smart contracts and blockchain technologies.

5.2.1 Our proposal in a nutshell

Figure 5.2 shows a general overview of the protocol's steps, along with their actors, related to the access control scenario and its posterior payment phase. In this layout, the involved actors, i.e. Drivers (D) and Access control infrastructure (AC), should obtain valid credentials from the LEZ Administrator (LA) in order to securely interact with other entities of the system. In case of D, the vehicle's OBU should obtain group signature credentials bound to its vehicle emissions category in order to certify this condition to the AC infrastructures. Furthermore, all entities interacting with the smart contract at some point of the protocol, i.e. D, AC and LA, should generate digital wallets for that purpose, which, in case of D, also includes her access payments to the LEZ.

The access scheme starts when D approaches to the LEZ entrance and her vehicle's OBU automatically initiates the protocol. The detection of *Bluetooth Low Energy* beacons can be, for instance, the trigger to automatize this process without D's intervention. On that awakening signal, D's OBU establishes a secure connection using a short-range communication system, e.g. Bluetooth, with the AC and, through an authentication process, demonstrates the vehicle's emissions category that D is driving.

By successfully concluding this process, AC and D can agree an access receipt, containing the entrance parameters, which act as proof of their

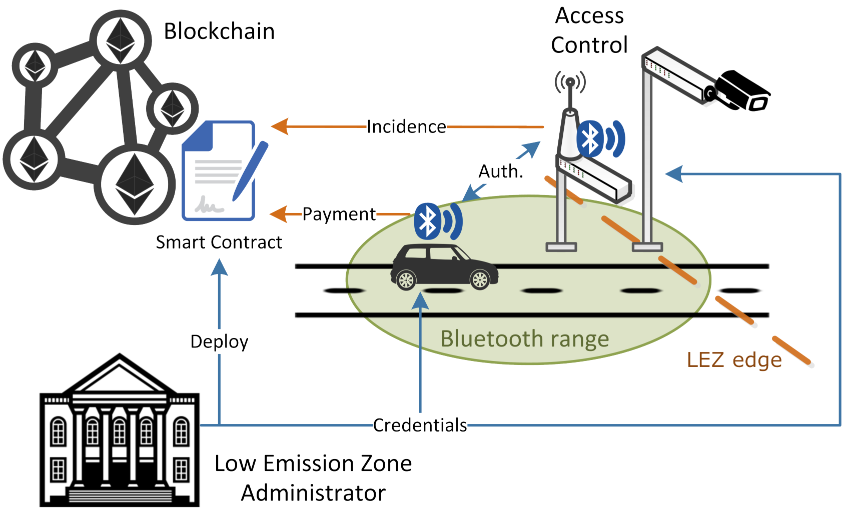


Figure 5.2: General scheme of the proposal

interaction. During the whole process D's privacy is preserved as all generated evidences are signed, due to our group signature scheme, on behalf of her vehicle's emissions category group. In this way, ACs, or the entities supporting them, are prevented from binding any of D accesses. Conversely, if the process fails due to D's dishonest behaviour, i.e. she tries to alter or skip parts of the protocol, AC will take a photo of the vehicle revealing its license plate and, thus, disclosing the driver's identity.

Once a valid access receipt is obtained, D can initiate the payment process by interacting with the deployed the LA-deployed smart contract. For this, D remotely calls the payment function of the smart contract, sending the agreed access data as parameters. On the basis of this information, the smart contract's logic verifies its validity and calculates the fee to pay according to the last uploaded prices list in the blockchain. If the access receipt is valid and it was issued by an LA-authorized AC, the corresponding amount of LEZ digital tokens is transferred from D's to AC's digital wallet.

When enough time elapsed for the access transaction being validated and added to the blockchain, the involved AC verifies the transaction's status to determine if the access payment was correctly conducted. In case any irregularity is found, e.g. the access transaction in not in the blockchain or its status is not set as "paid", AC interacts with the smart contract to publish an access incidence. In this process, the AC uploads to the blockchain its own access receipt copy, which not only contains the access details, but also D's group signature. With this information published, the LA, as the groups manager, can disclose D's identity and, thus, revoke her privacy.

5.2.2 Blockchain integration

The public ledger known as blockchain was originally designed as a mechanism to provide decentralization to financial transactions. The principle behind it consists in granting equal decentralized trust to any node with the power of solving computational challenges, known as proof-of-work, and using it as a way to reach consensus. This concept was extended in [28] with Ethereum, whereby programmable logic programs, referred to as smart contracts, are executed on the Blockchain permitting to decentrally settle transactions of arbitrary resources.

The presented proposal uses the programmable logic of Ethereum's smart contracts to include vehicle access details in blockchain transactions, and, on the basis of these data, automatically transfer its corresponding fee in terms of digital tokens. With this procedure, the nodes of the blockchain network are able to decentrally validate the vehicle access to the LEZ, allowing the system the omission of centralized third parties that oversee the whole process.

The blockchain paradigm requires that network nodes, known as miners, contribute with their computational resources to validate transactions and, further, a trustworthy advancement of the chain. In the proposed scenario, two entities are potentially incentivized to contribute in that task: i) LA, as the main provider of digital tokens and the most interested in their consumption; and ii) ACs and the entities behind them, as they receive monetary compensation from the tokens earned in each access transaction they participate in.

5.3 Protocol

Our system involves the four following actors: i) LEZ Administration (LA); ii) Drivers (D); iii) Access Control Infrastructure (AC); and iv) Cryptocurrency Mixing Service (M).

- LEZ Administration (LA): is the entity who is in charge of managing the LEZ and establishing the restrictions applied to the vehicles accessing this area. Among its tasks is to issue valid certificates to other system's entities and deploy the LEZ's smart contract.

- Drivers (D): are the potential users of the proposed scheme, who, when accessing the LEZ, interact with the system's infrastructures through the on-board units (OBU) embedded in their vehicles. OBUs are expected to be devices able to perform cryptographic operations, equipped with GPS technology, 4G, short range communication (e.g. Bluetooth) and a tamper-proof secure element (SE). It is assumed that SE already has the vehicle's license plate stored in it.

- Access Control (AC): are the infrastructures controlling the vehicle access to the LEZ. With this purpose, they are expected to be equipped with a camera, GPS, short range communication and Internet access. These infrastructures may be under control of one or more for-profit entities as long as the LA is not one of them.

- Cryptocurrency Mixing Service (M): is an independent entity in charge of obfuscate the tractability of blockchain transactions, so that transferred funds cannot be trailed back to the source digital wallet.

This section formalizes the different phases that drive the proposed system, giving enough detail to allow their implementation. These are:

- *On-board unit set-up*: it describes the registration process that a D's OBU should complete with the LA to obtain the needed credentials to successfully interact with the system.
- *Wallet filling*: it outlines the operations D should perform to anonymously purchase LEZ digital tokens, elements acting as native currency in our system, from LA.
- *Access*: it describes the interactions between D and AC to agree the parameters of an access to the LEZ.
- *Payment*: it defines the steps D should follow for publishing an agreed LEZ access to the blockchain and paying its corresponding amount by means of smart contract interaction. AC countermeasures against dishonest Ds, who try to alter the protocol for their own profit, are also described.

5.3.1 On-board unit set-up

The first protocol step the users should fulfill is registering into the system and obtaining the adequate credentials to successfully interact with the LEZ infrastructures. To this end, D's OBU establishes a secure communication channel, with the LA server and provides the vehicle data (plate number, car maker, model, etc.). The LA, as a governmental entity (e.g. city council), is able to verify the correctness of the vehicle's data and obtain the information of the vehicle's owner.

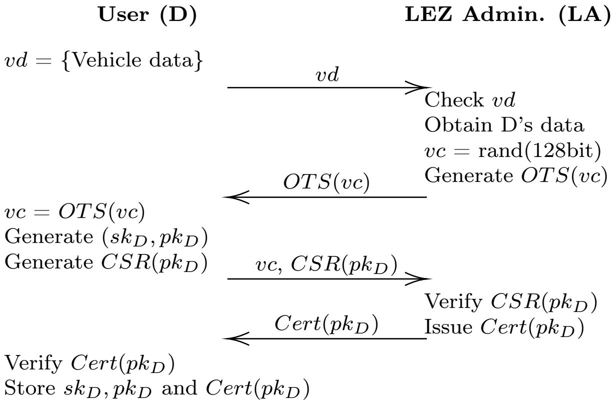
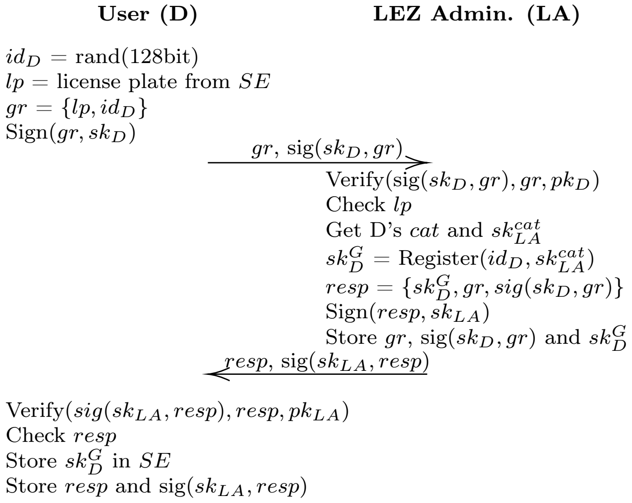


Figure 5.3: OBU set-up

Then, as steps in Figure 5.3 show, LA generates a 128-bit vehicle code vc and sends it as a One-Time-Secret (OTS) URL linked to D through a side channel (email, phone, etc.). D, once vc is retrieved, generates a key pair (sk_D, pk_D), a certificate signing request $CSR(pk_D)$, containing vc, and sends this last one back to LA. On the basis of $CSR(pk_D)$, LA verifies the validity of vc and issues its corresponding certificate $Cert(pk_D)$, including vc in the *CommonName* field and the vehicle emissions category *cat* as an extension. Finally, D checks the validity of the received certificate $Cert(pk_D)$ and stores the generated credentials.

Through the completion of the previous process, D obtains a valid LA-issued certificate $Cert(pk_D)$, which allows her to complete strong bilateral authentication with the other entities of the system. On this basis, D then establishes secure communication with LA, which comprises a two-way authentication. By means of this channel, LA and D are negotiating the group signature keys that D is using to validate her accesses. Figure 5.4 illustrates these steps.



User (D)

id_D = rand(128bit)
lp = license plate from SE
$gr = \{lp, id_D\}$
Sign(gr, sk_D)

$$\xrightarrow{gr,\ \text{sig}(sk_D, gr)}$$

LEZ Admin. (LA)

Verify(sig$(sk_D, gr), gr, pk_D)$
Check lp
Get D's cat and sk_{LA}^{cat}
sk_D^G = Register(id_D, sk_{LA}^{cat})
$resp = \{sk_D^G, gr, sig(sk_D, gr)\}$
Sign$(resp, sk_{LA})$
Store gr, sig(sk_D, gr) and sk_D^G

$$\xleftarrow{resp,\ \text{sig}(sk_{LA}, resp)}$$

Verify$(sig(sk_{LA}, resp), resp, pk_{LA})$
Check $resp$
Store sk_D^G in SE
Store $resp$ and sig$(sk_{LA}, resp)$

Figure 5.4: Group signature keys negotiation

D initiates the process preparing a key generation request gr which contains a random identifier id_D and a license plate proof lp, generated by SE. D signs this request with her private key Sign(gr, sk_D) before sending it to LA. When LA receives a request gr from D, first, verifies its signature. If it is correct, checks the validity of the license plate lp and verifies if it matches the vehicle behind the code vc contained in D's certificate $Cert(pk_D)$. Then, it selects the group private key sk_{LA}^{cat} associated with vehicle's emissions category and initiates the generation process. In this operation, LA, inputs sk_{LA}^{cat} and id_D to generate D's group private key sk_D^G. The exact steps of the *Register* process are detailed in Section 5.1 and [33]. Finally, a generation response *resp*, containing the generated key and the D's generation request, along with its signature is sent back to D. In the other end, D verifies the received response and stores all received data as proof of the generation process. sk_D^G is then stored in the SE of the OBU.

Once the credentials generation process is completed, D generates an Ethereum digital wallet W_D or, depending on her privacy preferences, a group of them $W_D^1..W_D^n$, as she is required to publish transactions on the blockchain for paying her access to the LEZ through the use of smart contracts. For this purpose, D generates a private key sk_D^W of 256-bit, a public key pk_D^W of 512-bit and its corresponding address according to Ethereum key specs, for each wallet she is creating.

5.3.2 Wallet filling

As the presented scheme contemplates the access fee payment with smart contracts, Ds should purchase LEZ Ethereum tokens, i.e. elements acting as native currency in our system, from LA for their monetary transactions. For this purpose, it is expected that LA hosts a specific Internet portal where users can buy tokens in exchange of money or cryptocurrencies, like Ether or Bitcoin. In this matter, tokens purchased via cryptocurrency payments are expected to be anonymous, contrary to classic payment mechanisms, e.g. credit card or wire transfer, which pose privacy threads for users as let the LA bind their bank account data to their digital wallet and, thus, to their blockchain transactions.

In order to tackle this problem, D creates a temporal wallet W_D^T, generating a private and public key pair and its corresponding address according to Ethereum key specs, in which the purchased LEZ tokens will be transferred once bought from LA web portal. Then, D asks the cryptocurrency mixing service (e.g., ETH-Mixer[1]) to transfer the funds from W_D^T to her actual wallet W_D or group of wallets $W_D^1..W_D^n$. M, by means of the mixing process, obscures the link generated between the source and destination

[1] ETH-Mixer, https://eth-mixer.com/

wallets when funds are transferred, preventing the LA from linking the LEZ tokens purchaser with her transactions on the blockchain.

On this matter, although the purchaser's identity cannot be linked to her wallet, the transactions that a wallet is involved in can be linked together through its address. In order to address this problem, D can proceed in two different ways. On the one hand, D may use only one wallet at a time, generating a new one each time she wants to sever the link between her transactions. The remaining funds in the old wallet can be transferred to the new one by means of M and the transaction obfuscation process it provides. On the other hand, D also has the option of distributing her funds in small different amounts among several one-use wallets. In this way, D fractionally pays her access to the LEZ using different wallets and disposing the already-used empty ones in the process. Note that this process requires some planning by the client device when distributing D's token funds among all her wallets, as it should be able to combine them to add up the charging required fee.

5.3.3 Access

When D wants to access the LEZ, she establishes communication with AC in order to validate her access. This validation process, via short range communication, agrees some parameters in order to manage the later transaction in the blockchain. The process begins the moment D enters the AC communication range. Then, both entities establish secure communication, via TLS, implying one-way authentication from AC; and perform the steps in Figure 5.5.

D starts the process by sending the access data *ad*, including her position, date, time, vehicle emission category, a random access id a_{id} and a AC-generated nonce N_{TLS} from the previous TLS handshake. This data is signed, by the OBU's SE, on behalf of D's emission category group in

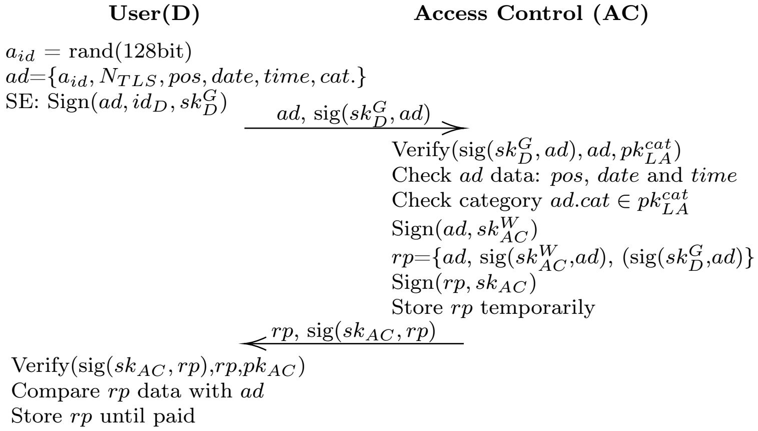

User(D)
Access Control (AC)
a_{id} = rand(128bit)
ad=$\{a_{id}, N_{TLS}, pos, date, time, cat.\}$
SE: Sign(ad, id_D, sk_D^G)
ad, sig(sk_D^G, ad)
Verify(sig(sk_D^G, ad)$, ad, pk_{LA}^{cat}$)
Check ad data: pos, $date$ and $time$
Check category $ad.cat \in pk_{LA}^{cat}$
Sign(ad, sk_{AC}^W)
rp=$\{ad$, sig(sk_{AC}^W,ad), (sig(sk_D^G,ad)$\}$
Sign(rp, sk_{AC})
Store rp temporarily
rp, sig(sk_{AC}, rp)
Verify(sig(sk_{AC}, rp),rp,pk_{AC})
Compare rp data with ad
Store rp until paid

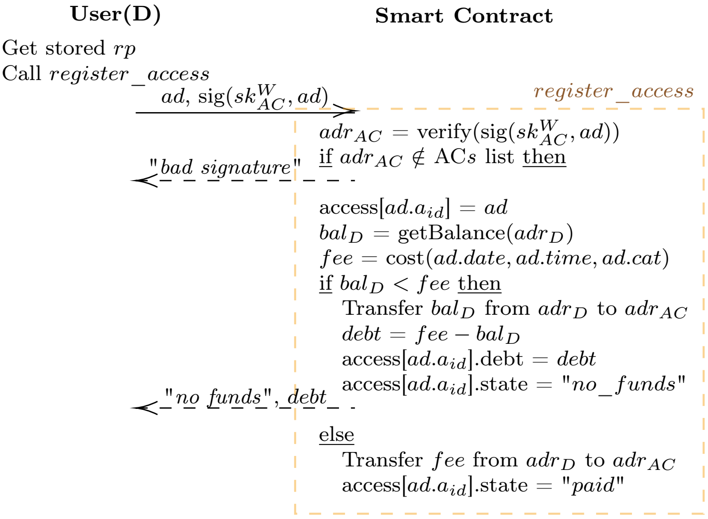
Figure 5.5: Access protocol

order to protect her privacy. On receipt of ad, AC verifies the correctness the data and its signature by means of the corresponding group public key pk_{LA}^{cat}. If verifications are correct, AC prepares an access receipt, which consists in the received data ad signed using AC's digital wallet private key sk_{AC}^W, so it can be verified on-chain by the LEZ smart contract. This signature is sent back to D along with the original received message, i.e. ad and its D's group signature, signed with AC's private key sk_{AC} as a proof of their access agreement. D temporally stores this proof once she contrasted the received data rp with the sent one ad and verified both AC's signatures. The exact steps of signature generation and verification processes are detailed in Section 5.1 and [33].

If at some point of this phase the user D fails to complete the authentication process by deliberately skipping or altering the protocol execution, the AC will take a photo of the vehicle's license plate. This photo will serve to identify the unauthenticated vehicle and, thus, revoke D's privacy.

5.3.4 Payment

Once AC and D agreed the entrance parameters and D obtained an access receipt *rp* from AC, the user can start the payment process of the access she has just registered. This process is managed through smart contracts, due to blockchain technology, without the intervention of centralized entities who acknowledge the user's movements. Namely, D, using the signed access receipt obtained from AC, interacts with the smart contract, which prices the access according to its parameters and automatically transfers the corresponding amount in terms of digital tokens. LA, which is assumed to be the smart contract's owner, has the authority to update the table of prices the smart contract inquires to determine the access fees. To do so, the LA interacts with the smart contract using the method *set_ prices* which uploads new prices to the blockchain.



```
$adr_{AC}$ = verify(sig($sk_{AC}^{W}$, $ad$))
if $adr_{AC} \notin$ ACs list then

access[$ad.a_{id}$] = $ad$
$bal_D$ = getBalance($adr_D$)
$fee$ = cost($ad.date, ad.time, ad.cat$)
if $bal_D < fee$ then
    Transfer $bal_D$ from $adr_D$ to $adr_{AC}$
    $debt = fee - bal_D$
    access[$ad.a_{id}$].debt = $debt$
    access[$ad.a_{id}$].state = "$no\_funds$"

else
    Transfer $fee$ from $adr_D$ to $adr_{AC}$
    access[$ad.a_{id}$].state = "$paid$"
```

Figure 5.6: Payment protocol: Payment

This process, shown, step by step, in Figure 5.6, starts when D interacts with the smart contract by invoking the *register_ access* method. On this process, D upload as parameters the access data *ad* and AC's digital wallet signature sig(sk_{AC}^{W},ad) contained in the access receipt *rp* received from AC. The smart contract, for its part, verifies on-chain the validity of AC's signature, as its signed using Ethereum protocol standards, and if its issuer is a valid AC registered in the smart contract. Then, on the basis of date, time and vehicle category, the access fee is calculated according to the last published prices in the blockchain and the corresponding amount is transferred from D's to AC's wallets in terms of LEZ tokens. In case of insufficient funds, the remaining amount is set as debt, so D can settle it using other wallets. Depending on the method outcome, access a_{id} status will be set a “bad signature", “no funds" or “paid". Once the status is set as “paid", no further action can be taken on this registered access.

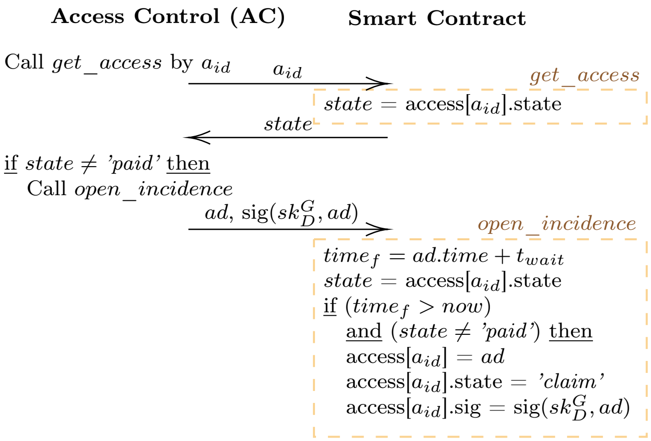

Access Control (AC)
Smart Contract
Call get_access by a_{id}
a_{id}
get_access
$state$ = access[a_{id}].state
$state$
if $state \neq$ 'paid' then
Call $open\_incidence$
ad, sig(sk_D^G, ad)
$open\_incidence$
$time_f = ad.time + t_{wait}$
$state$ = access[a_{id}].state
if ($time_f > now$)
and ($state \neq$ 'paid') then
access[a_{id}] = ad
access[a_{id}].state = 'claim'
access[a_{id}].sig = sig(sk_D^G, ad)

Figure 5.7: Payment protocol: Incidence claim

Later, once enough time elapsed for the access transaction being validated, AC verifies if a transaction a_{id} is published to the blockchain with “*paid*" status. AC can recover the access's state by invoking the *get_ access* smart contract method as shown in Figure 5.7. In case these conditions are not met, AC publishes an incidence to the blockchain calling the *open_incidence* method. D's access data and its signature on behalf of her vehicle emission category group are sent as parameters. The smart contract, on its part, verifies if the conditions to open an incidence are met and publish D's group signature if required. LA, as the owner of the smart contract, is in charge of establishing the time that must elapse for an incidence to be opened. With this procedure, LA has the means to identify D through her group signature, revoke her privacy and initiate sanctioning measures against her.

By following this process, AC*s* gather LEZ tokens in their wallets for every registered access. It is assumed that LA, at each billing period, will monetarily reward AC*s*, or the entities behind them, in accordance to the gathered token amount, thereby getting profit from their services.

5.4 Security and privacy analysis

The security requirements and how they are fulfilled is defined in this section. Bearing this in mind, the adversary model is introduced first, then security requirements are analyzed on a case-by-case basis.

For this approach the attacker model considers both internal and externals adversaries. As internal attackers, AC*s*, which are honest but curious, and dishonest D*s*, who try altering the protocol to commit fraud, are taken into account. On the other hand, any entity omitting the proposed protocols in order to commit fraud is considered as an external attacker. Finally, the LA, who acts as a certification authority, is fully trusted.

Considering this adversary model, the next sections explain the security properties of the presented system and how they are fulfilled.

- *Revocable anonymity.* Users' privacy is preserved as long as they do not try to commit fraud, in which case they can be identified even if they are outside the system.

- *User accesses are non-traceable and unlinkable.* User's actions cannot be bind together by third parties even when published to the blockchain.

- *Fraud avoidance.* A user cannot be falsely inquired about not completing a payment process.

- *Non-repudiation and integrity.* Evidences generated from entities interaction can be neither denied nor counterfeited.

5.4.1 Revocable anonymity

During the access phase, D is signing all her messages on behalf of her vehicle emission category group. As AC can only infer information from D's signatures, the only disclosed information from D to AC it is her vehicle emission category. In the payment phase, the access information is published to the blockchain under one of D's wallet address. As D's group signature is not published, neither internal nor external entities can disclose D identity.

Conversely, in the event of a dishonest user, skipping or altering the payment process to commit fraud, AC publishes its access receipt copy to the blockchain containing D's group signature. With this data, LA can disclose the group member behind the signature and initiate measures against her. In case a vehicle skips or fails to complete the access phase, AC takes a photo of its license plate, disclosing the driver's identity.

5.4.2 User accesses are non-traceable and unlinkable

AC*s* are only receiving access data and a randomized group signature in behalf of the emission category group from D. In that way, is not possible for AC*s* to bind any subsequent access of D. In the same vein, as D's group signature is only published to the blockchain in case of detecting a fraud attempt, neither the LA can link D's accesses.

During the payment phase, D is using several digital wallets, disposing empty ones, to unhook her involvement in previous blockchain transactions because of her wallet's address. New wallets can be generated at any point without the involvement of other entities.

When D is purchasing funds for her wallets from a non-anonymous source, she first transfers the bought tokens to a temporal wallet, from which will be transferred to the operative one. This last transaction is performed through a mixing service to obscure the transaction trail between the temporal wallet and the operative one. This way, the token retailer is not able to bind the purchaser information to her operating wallet.

5.4.3 Non-repudiation and integrity

In the access phase, both AC and D should prove they hold valid credentials issued by the LA. In this case, AC proofs its identify and D demonstrates that is a valid member of an emission category group. As a result of the access phase interaction, both AC and D receive an access receipt, containing the access details, signed by the counterparty; in case of D, her proof is signed in behalf of her emission category group. In both cases, signature validity can be verified by the counterparty, therefore, the proofs' integrity is granted. Also in both cases the signer identity can be disclosed, by means of LA in case of D's group signature, so the evidence generation cannot be denied.

5.4.4 Fraud avoidance

In order to open a fraud incidence against D, AC has to publish an access receipt with D's group signature in the blockchain. In that way, it is not possible for any AC to falsely accuse D, as the valid proof to support an incidence can only be obtained by successfully completing access process between the involved entities.

5.5 Experimental Results

In this section, we evaluate the performance of the protocol's phases subjected to real-time computing, i.e. phases whose feasibility is bound to strict temporal constraints. In our LEZ scenario, these restrictions are present between AC and D interaction during the Access phase, as vehicles have to finish this process while they are in range to communicate.

In order to perform this evaluation, we implemented the protocol steps described in Section 5.3.3 along with entities involved in the process: *D* and *AC*. Bearing this in mind, the AC is implemented on a Raspberry Pi 2 900MHz quad-core ARM Cortex-A7 CPU, 1GB RAM using Raspbian OS, and the protocol is written in Java7. On the client's side, D's OBU is impersonated by an Android application written in Java8 running on LG Nexus 5 with a Snapdragon 800, 2GB Ram and Android 6.0 OS. Finally, the OBU's SE, performing the group signature operations, is implemented in a ML4 smartcard 2KB RAM using Multos 4.1 OS and written in C. In this testbed, D's group signatures are performed using d224-sized elliptic curves. The rest of signatures and encryptions are computed using RSA scheme with 2048-bit key size.

In order to support our evaluation and to provide a fair comparison, we also implemented the Access phase steps of most similar approaches in the literature [16, 17, 29] and run testbeds under the same conditions.

Table 5.1: Computation time comparison in seconds

	Client side	AC side	Total
[29]	.083	.367	.450
Our scheme	.444	.594	1.038
[16]	1.321	.582	1.903
[17]	1.339	.662	2.001

5.5.1 Performance

As seen in Table 5.1, our protocol consumes in computation an average time of 1.038 seconds. More specifically, AC, who performs the most computational expensive operations, takes 0.594 seconds. Most of this time, 0.268, is spent in AC's RSA signature generation, followed by group signature verification process, which comprises costly bilinear pairing operations, taking 0.234 seconds. The remaining 0.092 seconds are spent in generating AC's digital wallet signature and other non-cryptographic operations. In this way, the driver-side is more lightweight and almost all of its 0.444 seconds are spent by the SE, which has lower computational power, for generating D's group signature. Putting that into perspective, this same signature process in the AC-side will only take 0.053 seconds.

Our proposal is especially suited for LEZs scenarios, as it stands for being lightweight on the client-side, which is composed by an OBU and its SE, and performing the most computational expensive operations on the AC-side, which can be embedded with greater CPUs.

5.5.2 Comparison

Table 5.1 shows the average times dedicated to computational tasks, during the access phase, by most similar schemes in the literature. As it can be seen, [29] is, with difference, the most lightweight protocol. However, it does not contemplate the use of a SE on the client side, which results in fast RSA signature generations, and bases users' privacy protection on pseudonyms, which reduces signature verification complexity at the expense of users' linkability. Regarding the other group-signature-based approaches, [16, 17], it draws special attention the times to complete their client computation. This is mainly caused because their clients are using 2048-bit RSA signatures that, due to their scheme design, can only be generated by the SE, posing the heaviest computational part on the slowest component.

Regarding our scheme, it achieves better times than the other group-signature schemes [16, 17] due to a more lightweight client protocol. In that way, costly bilinear pairing operations are performed during group-signature verification and, thus, executed on the AC-side. This allows a light signature process on the client-side that proves to be feasible even if executed in the OBU's SE.

Finally, it also should be bore in mind that in [29, 16, 17] a credential renewal process is needed to keep preserving the users' privacy and, until this new certificates are not generated, their accesses to the LEZ are linkable. In case of [16, 17] this process can take up to 10 seconds as it should be computed inside the SE.

In a nutshell, it can be stated that our system is more lightweight than other group-signature-based works in the literature, and can even compete with faster less privacy-preserving approaches based on pseudonyms. Furthermore, it fully provides unlikabilty and non-traceability features without needing to regenerate, after each access, the drivers' credentials for achieving it.

Chapter 6

Conclusions

6.1 Contributions

Low Emission Zones have emerged as a popular mechanism to regulate traffic jams and environmental pollution in the last years. The restrictions and surcharges to contaminating vehicles, correspondingly to their emissions, that these LEZ solutions propose have been recently adopted in large cities' downtowns around the world.

In the view of that trend, it has aroused the need to implement access control systems for LEZ which enables compliance with such vehicular restrictions. While the currently deployed LEZ solutions have proven to be feasible, they have also turned out to require numerous infrastructures such as road side units and vehicle equipment. Furthermore, they have also been criticized in the literature due to the relevant privacy threat that they represent to the drivers passing by. In particular, current deployed systems used to enforce LEZs strongly depend on the use of camera networks that track the drivers' whereabouts indiscriminately. Moreover, they have a strong dependence on centralized entities to manage the processes related to vehicles' access authorization and fee payment related processes, dependency that comprises the availability and security of the system as it poses a single point of failure.

For this reason, in this thesis we have contributed with three new Access Control schemes for LEZs which address the deployability and centralization issues that current works in the literature present, while preserving the privacy of honest users by means of a revocable anonymity paradigm.

In our first contribution, presented in Chapter 3, we have designed a system that allows controlling the access to LEZs in an anonymous, secure and efficient way. In contrast to other schemes, our system presents a non-probabilistic fraud control system which identifies dishonest users while preserves the privacy of the ones who behave honestly. The lightweight design and the use of widespread technologies have made possible the system's implementation in low-cost infrastructures and the use of smartphones as user's side devices. On the basis of this implementation, we presented experimental results that prove that our system is feasible in real scenarios as defined in TRL5 of technological maturity. Field results show that a vehicle circulating at maximum permitted speed inside an urban environment would travel a distance which can be easily covered by the low cost Bluetooth device build-in in our AC's infrastructure. Experiments also show that most of time is spent in communication issues as connection establishment. However, a significant drop in that aspect is expected when newer widespread versions of Bluetooth technology are used.

In Chapter 4 we presented our second contribution, a decentralized privacy-preserving alternative that sits on the non-probabilistic fraud control system from our first contribution. Our scheme introduces a new decentralized privacy-preserving approach for controlling the access to LEZ*s* whose fundamental principle is the adoption of the smart contract technology to omit central entities from payment related processes in favor of the decentralization that blockchain technology offers. In our approach, interactions between users and LEZ's infrastructures are processed as blockchain transactions, through the use of smart contracts, thereby permitting the corresponding access fees to be automatically calculated and charged from the user's wallet in terms of digital tokens. Under this procedure, entities responsible of registering vehicle accesses and charging their corresponding fees are replaced by a decentralized network, which grants the verifiability, reliability and transparency of the uploaded LEZ accesses. Furthermore, as any node belonging to the distributed network can verify the validity of the transaction flow and every vehicular access transaction is added to the blockchain, there is no need for entities to locally store signed proofs of every entrance to the LEZ.

Finally, as our third contribution, the access control system for LEZ proposed in Chapter 5 follows previous proposal's decentralized trend of omitting third parties from access data acknowledgment and payment related processes in favor of blockchain and smart contracts technologies. Unlike previous approaches, this scheme truly preserves the anonymity, non-traceability and unlikablility of honest users through an efficient tailored group signature scheme, without the need of a client-on-demand credential renewal process to achieve it. On top of that, experimental results show that our system is more lightweight than similar group-signature-based LEZ access control systems in the literature, and can even compete with faster approaches based on pseudonyms.

6.2 Publications

The publications supporting the content of this thesis are stated below:

1. Jordi Castellà-Roca, Macià Mut-Puigserver, M Magdalena Payeras-Capella, Alexandre Viejo and Carles Angles-Tafalla. "Secure and Anonymous Vehicle Access Control System to Traffic-Restricted Urban Areas". In *2017 26th International Conference on Computer Communication and Networks (ICCCN)* (pp. 1-7). IEEE.

2. Carles Anglès-Tafalla, Jordi Castella-Roca, Macià Mut-Puigserver, M Magdalena Payeras-Capella and Alexandre Viejo. "Secure and privacy-preserving lightweight access control system for low emission zones". *Computer Networks*, 145, 13-26. 1st Quartile (13/52), Hardware & Architecture, Impact factor 3.03.

3. Carles Anglès-Tafalla, Jordi Castellà-Roca and Alexandre Viejo. "Privacy-preserving and secure decentralized access control system for low emission zones". In *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (IEEE, 2019).*

4. Carles Anglès-Tafalla, Sara Ricci, Petr Dzurenda, Jan Hajny, Jordi Castellà-Roca and Alexandre Viejo. "Decentralized privacy-preserving access for low emission zones". In *Proceedings of the 16th International Joint Conference on e-Business and Telecommunications - Volume 2: SECRYPT*, 485-491. INSTICC (SciTePress, 2019).

6.3 Future Work

Regarding the contributions presented in this thesis, we foresee some open problems and extensions that will be addressed in the future.

Concerning our decentralized schemes, we plan to extend the proposed protocol to a more flexible approach in terms of fee calculation parameters. In view of the limitation of the current schemes to charge fees only per access, the intended breadth of the protocol it is expected to calculate the vehicle fees according to more accurate parameters, like the time elapsed or the distance traveled inside the restricted area.

In order to evaluate the performance of our decentralized approaches, we implemented the critical parts of the protocols that are bound to specific temporal constrains. However, a complete implementation of the proposed scheme is intended in order to validate the feasibility of the proposed schemes in a real world scenario. On the basis of this implementation, it is expected to evaluate the computational cost of the smart contract's logic in terms of gas consumption, i.e. a unit that measures the amount of computational effort that it will take to execute its operations. The knowledge of this metric is of great importance in order to determine the contract's deployability.

Bibliography

[1] Health Effects Institute Panel on the Health Effects of Traffic-Related Air Pollution, *Traffic-related air pollution: a critical review of the literature on emissions, exposure, and health effects.* No. 17, Health Effects Institute, 2010.

[2] R. Xie, D. Wei, F. Han, Y. Lu, J. Fang, Y. Liu, and J. Wang, "The effect of traffic density on smog pollution: evidence from chinese cities," *Technological Forecasting and Social Change*, vol. 144, pp. 421–427, 2019.

[3] World Health Organization and UNAIDS and others, *Air quality guidelines: global update 2005.* World Health Organization, 2006.

[4] R. J. Laumbach and H. M. Kipen, "Respiratory health effects of air pollution: update on biomass smoke and traffic pollution," *Journal of allergy and clinical immunology*, vol. 129, no. 1, pp. 3–11, 2012.

[5] R. M. Vivanco-Hidalgo, G. A. Wellenius, X. Basagaña, M. Cirach, A. G. González, P. de Ceballos, A. Zabalza, J. Jiménez-Conde, C. Soriano-Tarraga, E. Giralt-Steinhauer, *et al.*, "Short-term exposure to traffic-related air pollution and ischemic stroke onset in barcelona, spain," *Environmental research*, vol. 162, pp. 160–165, 2018.

[6] C. R. Knittel, D. L. Miller, and N. J. Sanders, "Caution, drivers! children present: Traffic, pollution, and infant health," *Review of Economics and Statistics*, vol. 98, no. 2, pp. 350–366, 2016.

[7] E. Rapaport, "The stockholm environmental zone, a method to curb air pollution from bus and truck traffic," *Transportation Research Part D: Transport and Environment*, vol. 7, no. 3, pp. 213–224, 2002.

[8] G. Santos, "Urban congestion charging: a comparison between london and singapore," *Transport Reviews*, vol. 25, no. 5, pp. 511–534, 2005.

[9] R. A. Popa, H. Balakrishnan, and A. J. Blumberg, "Vpriv: Protecting privacy in location-based vehicular services," 2009.

[10] X. Chen, G. Lenzini, S. Mauw, and J. Pang, "A group signature based electronic toll pricing system," in *2012 Seventh International Conference on Availability, Reliability and Security*, pp. 85–93, IEEE, 2012.

[11] J. Balasch, A. Rial, C. Troncoso, B. Preneel, I. Verbauwhede, and C. Geuens, "Pretp: Privacy-preserving electronic toll pricing.," in *USENIX Security Symposium*, vol. 10, pp. 63–78, 2010.

[12] S. Meiklejohn, K. Mowery, S. Checkoway, and H. Shacham, "The phantom tollbooth: Privacy-preserving electronic toll collection in the presence of driver collusion.," in *USENIX security symposium*, vol. 201, pp. 1–16, 2011.

[13] J. Day, Y. Huang, E. Knapp, and I. Goldberg, "Spectre: spot-checked private ecash tolling at roadside," in *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society*, pp. 61–68, 2011.

[14] F. D. Garcia, E. R. Verheul, and B. Jacobs, "Cell-based privacy-friendly roadpricing," *Computers & Mathematics with Applications*, vol. 65, no. 5, pp. 774–785, 2013.

[15] R. Jardí-Cedó, M. Mut-Puigserver, M. M. Payeras-Capellà, J. Castellà-Roca, and A. Viejo, "Electronic road pricing system for low emission zones to preserve driver privacy," in *International Conference on Modeling Decisions for Artificial Intelligence*, pp. 1–13, Springer, 2014.

[16] R. Jardí-Cedó, M. Mut-Puigserver, M. M. Payeras, J. Castella-Roca, and A. Viejo, "Time-based low emission zones preserving drivers' privacy," *Future Generation Computer Systems*, vol. 80, pp. 558–571, 2018.

[17] R. Jardí-Cedó, J. Castellà, and A. Viejo, "Privacy-preserving electronic road pricing system for low emission zones with dynamic pricing," *Security and Communication Networks*, vol. 9, pp. 3197–3218, 2016.

[18] M. Hoffmann, V. Fetzer, M. Nagel, A. Rupp, and R. Schwerdt, "P4TC - provably-secure yet practical privacy-preserving toll collection," *IACR Cryptology ePrint Archive*, vol. 2018, p. 1106, 2018.

[19] S. Bouchelaghem and M. Omar, "Reliable and secure distributed smart road pricing system for smart cities," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 5, pp. 1592–1603, 2018.

[20] X. Chen, G. Lenzini, S. Mauw, and J. Pang, "Design and formal analysis of a group signature based electronic toll pricing system.," *JoWUA*, vol. 4, no. 1, pp. 55–75, 2013.

[21] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Annual international cryptology conference*, pp. 213–229, Springer, 2001.

[22] D. Chaum and E. Van Heyst, "Group signatures," in *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 257–265, Springer, 1991.

[23] F. D. Garcia, E. R. Verheul, and B. Jacobs, "Cell-based roadpricing," in *European Public Key Infrastructure Workshop*, pp. 106–122, Springer, 2011.

[24] G. Hartung, M. Hoffmann, M. Nagel, and A. Rupp, "Bba+: Improving the security and applicability of privacy-preserving point collection," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1925–1942, ACM, 2017.

[25] J. Castella-Roca, M. Mut-Puigserver, M. M. Payeras-Capella, A. Viejo, and C. Angles-Tafalla, "Secure and anonymous vehicle access control system to traffic-restricted urban areas," in *Computer Communication and Networks (ICCCN), 2017 26th International Conference on*, pp. 1–7, IEEE, 2017.

[26] C. Anglès-Tafalla, J. Castellà-Roca, M. Mut-Puigserver, M. M. Payeras-Capellà, and A. Viejo, "Secure and privacy-preserving lightweight access control system for low emission zones," *Computer Networks*, vol. 145, pp. 13–26, 2018.

[27] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[28] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, pp. 1–32, 2014.

[29] C. Anglès-Tafalla, J. Castellà-Roca, and A. Viejo, "Privacy-preserving and secure decentralized access control system for low emission zones," in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, IEEE, 2019.

[30] D. Bayer, S. Haber, and W. S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," in *Sequences Ii*, pp. 329–334, Springer, 1993.

[31] R. C. Merkle, "A digital signature based on a conventional encryption function," in *Conference on the theory and application of cryptographic techniques*, pp. 369–378, Springer, 1987.

[32] C. Anglès-Tafalla, S. Ricci, P. Dzurenda, J. Hajny, J. Castellà-Roca, and A. Viejo, "Decentralized privacy-preserving access for low emission zones," in *Proceedings of the 16th International Joint Conference on e-Business and Telecommunications - Volume 2: SECRYPT,*, pp. 485–491, INSTICC, SciTePress, 2019.

[33] J. Hajny., P. Dzurenda., L. Malina., and S. Ricci., "Anonymous data collection scheme from short group signatures," in *Proceedings of the 15th International Joint Conference on e-Business and Telecommunications - Volume 1: SECRYPT,*, pp. 200–209, INSTICC, SciTePress, 2018.

[34] D. Boneh and X. Boyen, "Short signatures without random oracles and the sdh assumption in bilinear groups," *Journal of Cryptology*, vol. 21, no. 2, pp. 149–177, 2008.

[35] J. Camenisch, M. Drijvers, and J. Hajny, "Scalable revocation scheme for anonymous credentials based on n-times unlinkable proofs," in *Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society*, pp. 123–133, ACM, 2016.

[36] C.-P. Schnorr, "Efficient signature generation by smart cards," *Journal of cryptology*, vol. 4, no. 3, pp. 161–174, 1991.

UNIVERSITAT
ROVIRA i VIRGILI