IOTA-VPKI: a DLT-based and Resource Efficient Vehicular Public Key Infrastructure

Andrea Tesei, Luca Di Mauro, Mariano Falcitelli, Sandro Noto, Paolo Pagano
CNIT - National Inter-University Consortium for Telecommunications
{andrea.tesei, luca.dimauro, mariano.falcitelli, sandro.noto, paolo.pagano}@cnit.it

***Abstract*—Intelligent Transport Systems (ITS) show many potential benefits to the way we travel today. The security requirements to be matched in this kind of systems are challenging and they show technical, societal, legal, and economical concerns (e.g. anonymity, accountability, non-repudiation). To address security, standardization bodies (IEEE 1609.2, ETSI) and harmonization efforts (Car2Car Communication Consortium (C2C-CC)) have proposed a Certification Authority-based (CA-based) Vehicular Public Key Infrastructure (VPKI) which still suffers of Single Point of Failure (SPoF) locate in CAs and does not provide transparency in the certificate issuance.**

We propose IOTA-VPKI, a Distributed Ledger Technology-based (DLT-based) VPKI that improve the state-of-the-art eliminating SPoF with seamless scalability with respect to the users. IOTA-VPKI also guarantees transparency in the issuance of certificates as well as historical proof-of-possession by storing signed and hashed certificates on the IOTA ledger to facilitate verification procedure. The use of IOTA DLT assure also the feasible deploy in Internet of Things (IoT) domain, where the devices involved have limited computational resources. The effectiveness of our DLT-based VPKI will be measured in testbed for EU Horizon 2020-funded AUTOmated driving Progressed by Internet Of Things (AUTOPILOT) project.

***Index Terms*—Vehicular Communications, Security, Distributed Ledger Technology, Vehicular PKI, Blockchain-based PKI**

I. Introduction

In the last years of academic and industrial research it has been shown that the incorporation of information and communication technologies within vehicles and transportation infrastructure will revolutionize the way we travel today [1]. Cooperative Intelligent Transportation Systems (C-ITS) technologies and standards act as frameworks that enable a set of applications in the domain of road safety, traffic efficiency and driver assistance. The resulting network is mainly composed by *On-Board Units* (OBUs) installed in vehicles, and *Roadside Units* (RSUs) deployed on the road, to enable V2X communications (namely *Vehicular-to-Infrastructure* and *Vehicle-to-Vehicle* communications). Despite the many potential benefits of C-ITS, there are still critical challenges in the field of reliable and real-time communication between vehicles and transport infrastructure. Moreover, since all research activities within C-ITS aim to enhance safety and efficiency of transportation systems, specific security mechanisms are critical for a real-life deployment [3]. The selected security mechanisms have to match the challenging C-ITS security requirements showing technical, societal, legal, and economical concerns (e.g. privacy, unlinkability, anonymity). According to [2] and [10], in the last few years standardization bodies (IEEE 1609.2 WG [4] and ETSI with TS 102 940 [5], TS 102 941 [7] and TS 103 097 [8]) and harmonization efforts (Car2Car Communication Consortium (C2C-CC) [9]) have worked to reach a consensus to use a Vehicular Public Key Infrastructure (VPKI) [2] to match security requirements of a vehicular network. Besides the amount of research in the field of VPKI, several problems have been pointed out concerning misbehavior and cyber attacks in general (e.g. sybil attacks [17] or Distributed Denial of Service (DDoS) [2]). CA-based PKIs architecture have Single Point of Failure (SPoF) in CAs and they are vulnerable to CAs' errors or breaches that can allow misuse of credentials. Moreover CA-based PKIs mainly handle revocation with Certificate Revocation Lists (CRLs): this process can be costly in terms of time with consequently quite long update time of these lists. A new emerging approach to the development of PKI is to use Distributed Ledger Technologies (DLT), especially using specific DLT implementation known as *blockchain* [18], [19]. The basic idea is to use the fundamental architecture of *blockchain* together with its basic function as public and append-only distributed log to implement and enable the PKI functions (registration, update, revocation). Blockchain is well-suited to PKI and provide all features to eliminate SPoF, guarantee certificate transparency and revocation, and assure a reliable transaction record [11]. However the majority of the proposed blockchain-based PKI schemas are tied to Bitcoin structure (Bitcoin - Satoshi Nakamoto' cryptocurrency [20]) and this oblige to *trust* a set of miners to guarantee continuous confirmation of new blocks. On the one hand, blockchain-based PKI solve SPoF problem with its distributed structure; on the other hand the Bitcoin base protocol lead to such an *oligarchy* of miners, hence the resulting PKI can suffer of misbehavior that can be set up to lower its efficiency. Moreover the fluctuation of the price and fees of the corresponding cryptocurrency can lead to unpredictable costs of certificate load/update processes, and even the growth of the blockchain size replicated to each node is not reasonable in the Internet of Things (IoT) domain.

This project has received funding from the European Unions Horizon 2020 research and innovation programme under grant agreement No 731993, also referred as AUTOPILOT (AUTOmated driving Progressed by the Internet Of Things).

A. Contributions of this paper

We propose here a VPKI based on IOTA [21] (IOTA-VPKI), a revolutionary new, next generation public distributed ledger that do not use blocks, nor chain and also no miners. The IOTA wallet is protected by a *seed*, a 81 characters length string which acts like a private key to open the wallet. IOTA uses a novel invention called *Tangle* [22] which is based on Direct Acyclic Graph (DAG), where each node is a single transaction. The edge set of the Tangle is obtained in the following way: when a new transaction arrives, it must approve two previous transactions [22]. This is the reason why IOTA does not need miners: to issue a transaction, users must work to approve other transactions and therefore contribute to the network' security [22]. IOTA transaction are feeless: the actual "fee" is the work that each user must do to approve other transactions during issuing process. The Proof-of-Work (PoW) algorithm used in IOTA for spam protection is a short computational operation, which can be completed even in devices with limited resources (e.g. IoT domain). There is also the "genesis" transaction which is approved either directly or indirectly by all other transactions. The consensus on the Tangle is now guaranteed by the so called Coordinator, an entity controlled by the IOTA Foundation which issues zero-valued transactions every two minutes (i.e. *Milestones*). IOTA Foundation claims that whenever the public transaction traffic will reach a certain stable rate, they will shutdown the Coordinator and so IOTA will reach the fully distributed status. Our main contribution stands in the adaptation of SECMACE architecture proposed in [2] to set up a new generation VPKI based on a DLT implementation that was designed specifically for the IoT industry (IOTA DLT [22]) and does not oblige the use of miners and huge computational resources to actually issue transactions (namely to implement PKI functionality). IOTA supports also *Masked Authenticated Message* (MAM) channels, which can be used to exchange secured and encrypted messages using IOTA ledger. The IOTA-VPKI architecture is depicted in Fig. 1. On the one hand we mantain the main component of the VPKI proposed in [2], which are compliant with the C-ITS security standards. On the other hand, we embrace the DLT basic principles to map the PKI functions using IOTA implementation. Our proposed architecture will enhance SECMACE by removing the SPoF present in CAs with the help of IOTA distributed ledger. IOTA-VPKI guarantees also transparency in certificate issuance and a modification of certificate verification process done through IOTA ledger. To the best of our knowledge, this is the first proposed schema for a DLT-DAG-based VPKI that can be deployed in IoT domain applications with limited computational resources. We are also setting up a VKPI testbed for EU Horizon 2020-funded *AUTOmated driving Progressed by Internet Of Things* (AUTOPILOT) project [32]. The rest of the paper is organized as follows: in Section II we briefly describe relevant background about SECMACE system and DLTs; in Section III we present the relate work; we describe our main contribution IOTA-VPKI in Section IV; with Section V we conclude presenting conclusions and future work.

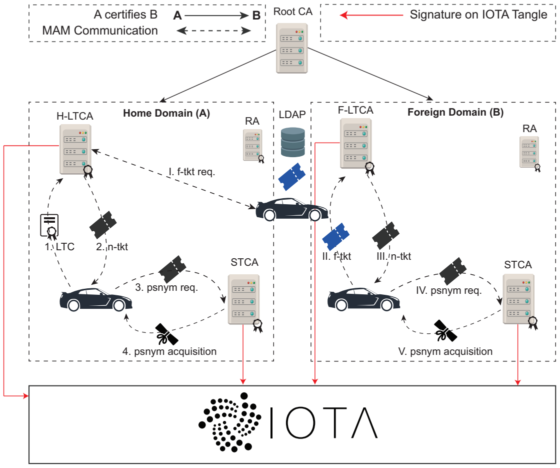

Fig. 1. IOTA-VPKI Architecture.

II. Background

A. SECMACE: the IOTA-VPKI building block

First presented in [2], SECMACE is a VPKI system compatible with standards ETSI [5], IEEE [4] and C2C-CC [9]. SECMACE implements standards with particular attention to *unlinkability* and *anonymity* of VPKI entities.

The authors assume that a VPKI is composed by a set of authorities with distinct roles [2]: the Root CA (RCA) as the highest-level authority which certifies lower-level authorities; the LTCA is responsible for vehicle registration and LTC issuance; the STCA (named Pseudonym CA (PCA) in [2]) is responsible for issues pseudonyms for registered and trusted vehicles; and Resolution Authority (RA) can to initiate a process to resolve a pseudonym to a LTC identity of misbehaving, malfunctioning, or outdated vehicle. The authors further divide the architecture in two different *domains*: an *Home domain* as the one that contains the Home LTCA (H-LTCA) where the vehicle are registered from the beginning; a *Foreign domain* as the one which a vehicle can reach after leaving its *Home domain*. A *domain* is defined as a set of vehicles, registered with their H-LTCA, subject to the same administrative regulations and policies [2]. Furthermore, all vehicles registered in the system are provided with HSMs: this assure the compliance with new standards update on security architecture and certificate formats (ETSI TS 102 940 v2.0.7 (2018-03) [6] and ETSI TS 103 097 v1.3.1 [8]).

Moreover, rather than assuming fully trustworthy VPKI entities, the authors assume an adversarial model in which these entities are considered *honest-but-curious*, i.e. multiple VPKI servers collude to harm users privacy [2].

B. Distributed Ledger Technologies

Ledgers have been at the heart of commerce since ancient times and are used to record most commonly assets like money and property. Paper-based ledgers have been substituted by digital one over the years, and nowadays one of the most prominent and potentially disruptive technology is called *Distributed Ledger Technology (DLT)*. Underlying this technology is the well known 'blockchain', which was invented to create the peer-to-peer cryptocurrency Bitcoin in 2008 [20]. The blockchain is a public ledger to which events are posted and verified by network members before being confirmed, i.e. *mined*. To append a new block to the chain, *miners* must compete to complete some Proof-of-Work (PoW) which usually is a cryptographic challenge. Besides the huge innovation of Bitcoin technology, several issues and threats has been discovered during its utilization (e.g. scalability, transaction speed, Goldfinger attacks) [31]. The second generation of blockchain technologies (e.g. Ethereum, Litecoin) tried to overcomes discovered issues. Despite the new interesting feature introduced in the second blockchain generation (namely *Smart Contracts* [28]), scalability as well as Goldfinger attacks are still present.

During the last years have been proposed several implementation of what is considered the third blockchain generation: DAG-based blockchain. No more chain of blocks: each node is a single transaction and edges represent *confirmation* of a single transaction. This new underlying ledger structure guarantees high level of scalability with respect to previous generation. Thanks to this structure and new confirmation protocols, some implementation can also assures resistance to quantum computing attacks and feeless transactions (e.g. IOTA [22]).

III. Related Work

As introduced in Section I, standardization bodies [4], [5], and harmonization efforts [9] have reached a consensus to use VPKI to protect C-ITS systems. The ETSI PKI architecture is depicted in Fig. 2. The key concept behind the proposed VPKI schema is the availability of two different public key certificates: a Long Term Certificate (LTC) (named Enrolment Certificate in ETSI standards [5]) is used to uniquely identify the vehicle; a Short Term Certificate (STC) or *pseudonym* (named Authorization Ticket (AT) in ETSI standards [5]) is used to grant specific services and permissions to a trusted and authenticated vehicle. The STC guarantees anonymous access to C-ITS communications and services and assure the unlinkability of messages originating from the vehicle [2]. Hence the system mantains a mapping of *pseudonyms* to the LTC for accountability and non-repudiation requirements. In order to manage these two types of certificate, the resulting VPKI is composed by two types of Certification Authorities (CAs): a Long Term CA (LTCA) (named Enrolment Authority (EA) in ETSI standards [5]) responsible for issuing LTCs to trusted vehicles; and a Short Term CA (STCA) (named Authorization Authority (AA) in ETSI standards [5]) responsible for issuing STCs to registered and trusted vehicles. Finally one or more Root CA acts as the trust anchor for the resulting VPKI, provide certificates to LTCA and STCA [10].

Each ITS Station (ITS-S) that wants to send a message has to acquire rights to access C-ITS communications from one LTCA (responsible for issuing its LTC). It negotiates then rights to invoke C-ITS services from STCA (namely receiving the *pseudonym* related to the requested services). Finally it digitally sign the message, e.g. Cooperative Awareness Messages (CAMs) or Decentralized Environmental Notification Messages (DENMs), with its private key k_v^i (corresponding to the currently valid *pseudonym* P_v^i), and finally sends the message if and only if all the previous steps end with success (namely the vehicle is considered *registered* and *trusted*). Sender ITS-S must attach its *pseudonym* to each message to facilitate the verification by any recipient. The way *pseudonyms* are constructed guarantees unlinkability and anonymity to VPKI users in valid messages [2], [3], [10].

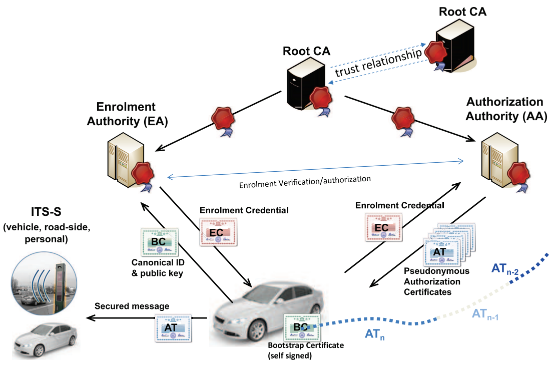

Fig. 2. ETSI PKI Architecture [5].

From the research point of view, there are many existing proposals for a VPKI. To the best of our knowledge, the most promising architecture is SECMACE [2] which is used as the base of our contribution. As explained in II-A, the authors propose an architecture that contributes a set of novel features: multi-domain operation, i.e. the distinction between *Home* and *Foreign* domain and all associated operations; increased user privacy protection by eliminating pseudonym linking based on timing information, considering also the presence of *honest-but-curious* system entities that can collude; prevent Sybil-based misbehavior; and multiple pseudonym acquisition policies.

In [25], [26], and [27] a ticket based approach was proposed. In these schemas the LTCA issues authenticated, yet anonymized, tickets for vehicles to obtain pseudonyms from STCA, with no direct communication between LTCA and STCA. However the LTCA can still learn the PCA from which the vehicle will receive pseudonyms, cause this information will be presented by the vehicle to the LTCA. Furthermore, the pseudonym acquisition period can be used to infer the active vehicle operation period as well as rough location of the vehicle. In [13] a proxy-based approach is used to let LTCA aggregates and shuffles all requests within a large period of time before forwarding them to the STCA: in this way the targeted STCA cannot identify which pseudonyms belong to which vehicles. Apart from the standards specifications, other approaches used to anonymous authentication are Group

Signature (GS) as proposed in [15] and [16]. One emerging approach is to use Blockchain technologies to implement distributed PKI. In Certcoin [19] a blockchain-based PKI not privacy-aware is proposed. In this schema the blockchain forms a ledger to which identity and public key are posted in pairs, along with the action (registration, update, revocation), and processed through verification and mining by the network. In Privacy-aware Blockchain-based PKI (PB-PKI) [11] the authors pointed out that in Certcoin is possible to link any public key to its owner at any time, because of the update process that is done posting the new public key in the online ledger. In PB-PKI once an identity is established, its key updates are anonymous unless the owner of such identity chooses to reveal them. This hidden linking is enabled by the offline secret key, used to prove the ownership of the public key when needed. However, these schema is based on Bitcoin implementation [20] and proof-of-work algorithm: this lead to a huge computational effort needed to perform transactions, i.e. save certificates on public ledger. In [23] a smart contact-based PKI is proposed, using Ethereum [28] blockchain technology. In this scheme there are two main components: the smart contract, which dictates the protocol of the system and acts as interface to the blockchain for the management of identities and attributes, as well as the client; and InterPlanerary File System (IPFS) [23] to allow users to fully utilise the system by allowing them to search for and filter attributes and identities. in [12] another Ethereum-based PKI management framework is proposed. Another approach is the Blockchain Authentication and Trust Module (BATM) proposed in [29]. BATM work starts from the idea of Pretty Good Privacy (PGP) [30] which use PKI to provide three main functionalities: confidentiality and encryption; authentication via digital signature; web of trust via identity validation from peers. BATM proposes a new way to achieve these goals using the blockchain as the database to store public keys, digital signature and peer information, allowing each component of the network to validate information about every other node in the network. However, in all blockchain-based schemas discussed here there are variable costs related to the use of the underlying blockchain technology due to fluctuation price of the cryptocurrency. Furthermore, all these schemas need the presence of a set of miners to allow performing transactions, i.e. saving identities on ledger. This leads to such an *oligarchy* of the set of miners that can misbehave and produce disruption of the service.

IV. IOTA-VPKI: IOTA-BASED VEHICULAR PKI

A. Architecture Overview

IOTA-VPKI is a DLT-based adaptation of SECMACE VPKI, a credential management infrastructure proposed in [2]. As described in section II-A, SECMACE is compliant with the common security architecture of C-ITS agreed by standardization bodies and harmonization efforts (namely IEEE1609.2 WG [4], ETSI [5], C2C-CC [9]).

Besides the many improvements done by SECMACE in terms of VPKI security (e.g. preventing Sybil-based misbehavior, unlinkability of pseudonyms), the proposed schema still follows the CA-based one. Hence the resulting VPKI has all known issues of this kind of credential management system described in section I. Starting from this, we use the DLT implementation called IOTA to overcome these issues, implementing VPKI operations and functionality directly using IOTA *Tangle* Ledger. As introduced in I-A, IOTA is a DAG-based DLT implementation well suited for IoT domain. Devices with small resource capacity can issue a transaction by communicating with the nearest neighbor IOTA Reference Implementation node (IRI). IRI nodes allow all devices to communicate with the peer-to-peer network that the Tangle operates on. IOTA implementation also offers *Masked Authenticated Message* (MAM) channels that implement IoT data flow management. The channel owner publishes new data on its channel; viewers subscribe to the channel to get data that is available. This ownership is implemented and secured in IOTA by a *seed*. There are three mode for MAM channels:

- *Public*: everyone can view the data;
- *Private*: only the owner can view the data;
- *Restricted*: data is protected by a *key*, and owner gives this key only to authorized viewers.

The main drawback of current MAM channel implementation stands behind the need to store messages in *Permanodes* to prevent deletion. This kind of nodes requires large storage, bandwidth and high speed, so they cannot be hosted on devices with small computational resources.

In our schema, the functionality, VPKI entities and their interactions are the same as in SECMACE infrastructure. We assume that each CAs (LTCA or STCA) has its own IOTA wallet with the corresponding *seed* and it has also a MAM encrypted channel (*Restricted* channel mode) to assure confidentiality in registration and update certificate procedures. As depicted in Fig. 1 the communication represented by dashed line connector are sent with MAM secure channels and they are used for end-to-end secure communication between CAs (LTCA or STCA) and vehicles. To enhance security, an IRI node can be deployed by the CA owners in order to avoid man-in-the-middle (MITM) attacks while issuing transactions.

During the registration phase, each vehicle negotiate a symmetric key with its H-LTCA that will be used in end-to-end encrypted communications within MAM channel. Even in presence of multiple instances of H-LTCAs (e.g. for scalability reasons), each vehicle will continue to use the same known MAM channel.

The use of IOTA DLT eliminates the SPoF in CAs as they can be replicated transparently with respect to the vehicle point of view: whenever a new instance of a given CA is deployed, it receives a copy of the *seed* by the first CA instance. This enables the new CA instance to manage the same *wallet* as well as the same MAM channels. Existing registered vehicles are not aware of how many CA instances are active: they will continue to use the same MAM channels with corresponding symmetric keys. This leads to a VPKI that is resistant to DDoS attacks and the availability level can be much higher than normal CA-based PKI even in presence of these attacks.

Moreover, IOTA guarantees integrity of the messages thanks to its protocol which is guaranteed even in the presence of quantum computer attacks. We further enhance other proposals described in Section II as we have based our approach on IOTA which is specifically suited for IoT Industry and the operations needed to interact with IOTA ledger (namely *The Tangle* [22]) can be executed on devices with limited computational resources.

B. Certificate Verification in IOTA-VPKI

We have introduced then an additional step in the ticket and pseudonym provisioning protocols described in [2]: at the end of provisioning process, we make the involved CA posts on IOTA ledger a special signature of the hash of the issued certificate, giving back to the vehicle the address on the ledger where this signature is. Then the vehicle attach the received IOTA ledger address to the messages that it is willing to send, so that any recipient can verify the validity and trust of the received message by directly access to the IOTA ledger. This additional step acts as an *historical proof* of the valid issuance of all the certificate. This additional step assure also that nobody can steal the certificate with the information available on the ledger because only the hash value of the certificate is publicly available to every VPKI entities.

In addition to the SECMACE' operations described in Section II-A, the CA issuing the certificate (LTC or STC) posts on the IOTA ledger the following signature:

$$S = (Sign(Lk_{CA}, H(crt)), Id_{CA}) \tag{1}$$

Where:

- Lk_{CA}: is the private key of the CA that has issued the given *crt*;
- H: is a cryptographic hash functions that guarantees the integrity of the certificate value;
- *crt*: the issued certificate;
- Id_{CA}: the ID of the CA that has issued the given certificate (e.g. for transparency of certificates issuance).

The signature S will be saved on the IOTA ledger to be accessed during verification of the integrity and validity of each message signed with *crt*. Moreover, this signature does not limit the anonymity of the VPKI entities thanks to the use of a cryptographic hash function given that is infeasible to invert the hashed value and obtain the original certificate to trace a VPKI entity. Id_{CA} is attached to the signature to add information about the signer CA. All instances of H-LTCA and PCA have to publish this signature on the online ledger each time they issue a new certificate or update an existing one.

V. Future Work and Conclusions

Nowadays C-ITS is considered one of the most prominent technology which will revolutionize the way we travel today. Standardization bodies and harmonization efforts have reached a consensus to use VPKI to protect these systems. However, the available proposals are mainly CA-based VPKI which suffers from SPoF, scalability problem and transparency of issuance of certificates. To address the existing limits, we proposed IOTA-VPKI, a DLT-based VPKI backed by IOTA DLT implementation. IOTA is the first open-source distributed ledger that is being built to be executed on devices with limited computational resources (e.g. IoT devices). IOTA-VPKI improves upon prior art in terms of scalability, absence of SPoF, and enhancing in transparency of issuances with a novel certificate verification protocol which guarantees integrity and historical proof of certificate validity.

As future work, we are setting up a IOTA-VPKI testbed for AUTOPILOT H2020-funded project to perform extensive tests on the effectiveness of the proposed approach, as well as performance tests. We intend to investigate how to map other C-ITS operations within the distributed ledger (e.g. V2X messages sent through IOTA ledger). Another possible extension is related to RA: with the help of LTCA and STCA, the RA entity present in SECMACE can be implemented by let it analyze the content of the distributed ledger, and retrieve the identity of misbehaving ITS-S.

References

[1] A. Muhammad, J. Ferreira, and J. Fonseca, eds. "Intelligent transportation systems: Dependable vehicular communications for improved road safety". Vol. 52. Springer, 2016.

[2] M. Khodaei, H. Jin, and P. Papadimitratos. "SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems." arXiv preprint arXiv:1707.05518 (2017).

[3] P. Papadimitratos, V. Gligor, and J-P. Hubaux. "Securing vehicular communications-assumptions, requirements, and principles." (2006): 5-14.

[4] "IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages" IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013) (2016)

[5] ETSI, TS. "102 940 v1.2.1-Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management." Technical specification, European Telecommunications Standards Institute (2016).

[6] ETSI, TS. "Draft-102 940 v2.0.7 (2018-03)-Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management." Technical specification, European Telecommunications Standards Institute (2018).

[7] ETSI, TS. "102 941 V1.1.1-Intelligent Transport Systems (ITS); Security; Trust and Privacy Management." Standard, TC C-ITS (2012).

[8] ETSI, TS. "103 097 v1.3.1-Intelligent Transport Systems (ITS); Security; Security header and certificate formats." Technical specification, European Telecommunications Standards Institute (2017).

[9] Car2Car Communication Consortium, https://www.car-2-car.org

[10] B. Lonc, and P. Cincilla. "Cooperative its security framework: Standards and implementations progress in europe." In World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2016 IEEE 17th International Symposium on A, pp. 1-6. IEEE, 2016.

[11] L. Axon, and M. Goldsmith. "PB-PKI: a privacy-aware blockchain-based PKI." (2016).

[12] A. Yakubov, W. Shbair, A. Wallbom, and D. Sanda, "A Blockchain-Based PKI Management Framework". In The First IEEE/IFIP International Workshop on Managing and Managed by Blockchain (Man2Block) colocated with IEEE/IFIP NOMS 2018, Tapei, Tawain 23-27 April 2018.

[13] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn. "A security credential management system for V2V communications". in IEEE VNC, Boston, MA, USA, pp. 18, Dec. 2013

[14] D. Förster, H. Löhr, and F. Kargl, "PUCA: A Pseudonym Scheme with User-Controlled Anonymity for Vehicular Ad-Hoc Networks (VANET)" in IEEE VNC, Paderborn, Germany, Dec. 2014.

[15] D. Boneh, and H. Shacham, "Group Signatures with Verifier-Local Revocation" in Proceedings of the 11th ACM conference on Computer and communications security, Washington, DC, USA, Oct. 2004.

[16] D. Boneh, X. Boyen, and H. Shacham, “Short Group Signatures” in Proceedings of 24th Annual International Cryptology Conference, Santa Barbara, California, USA, Aug. 2004.

[17] J. R. Douceur, “The Sybil Attack” in ACM Peer-to-peer Systems, London, UK, Mar. 2002.

[18] Namecoin, https://namecoin.info, accessed on 20-05-2018 at 9:40.

[19] C. Fromknecht, D. Velicanu, and S. Yakoubov. “A Decentralized Public Key Infrastructure with Identity Retention.” IACR Cryptology ePrint Archive, 2014, 803.

[20] S. Nakamoto. “Bitcoin: A peer-to-peer electronic cash system.” (2008).

[21] IOTA, https://www.iota.org, accessed on 20-May-2018 at 12:30.

[22] S. Popov. “The Tangle.” url: https://iota.org/IOTA_Whitepaper.pdf (2018).

[23] M, Al-Bassam. “SCPKI: a smart contract-based PKI and identity system.” Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts. ACM, 2017.

[24] “Preparing Secure Vehicle-to-X Communication Systems - PRESERVE” Accessed Date: 20-May-2018. [Online]. Available: http://www.preserve-project.eu/

[25] N. Alexiou, M. Lagana‘, S. Gisdakis, M. Khodaei, and P. Papadimitratos, “VeSPA: Vehicular Security and Privacy-preserving Architecture” in ACM HotWiSec, Budapest, Hungary, Apr. 2013.

[26] N. Bimeyer, J. Petit, and K. M. Bayarou, “CoPRA: Conditional Pseudonym Resolution Algorithm in VANETs” in IEEE WONS, Banff, Canada, pp. 916, Mar. 2013.

[27] S. Gisdakis, M. Lagana‘, T. Giannetsos, and P. Papadimitratos, “SEROSA: SERvice Oriented Security Architecture for Vehicular Communications” in IEEE VNC, Boston, MA, USA, Dec. 2013.

[28] G. Wood, “Ethereum: A secure decentralised generalised transaction ledger.” Ethereum project yellow paper 151 (2014).

[29] A. Moinet, D. Benoît, and B. Jean-Luc. “Blockchain based trust & authentication for decentralized sensor networks.” arXiv preprint arXiv:1706.01730 (2017).

[30] P. Zimmerman, “Pretty good privacy” 1991

[31] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten. “Sok: Research perspectives and challenges for bitcoin and cryptocurrencies.” In Security and Privacy (SP), 2015 IEEE Symposium on, pp. 104-121. IEEE, 2015.

[32] AUTOPILOT project, http://www.autopilot-project.eu/, accessed on 23-May-2018 at 12:30.