Auditable De-anonymization in V2X Communication

Masoud Naderpour[1], Tommi Meskanen[1], Andrew Paverd[2] and Valtteri Niemi[1]

[1]*Department of Computer Science, University of Helsinki, Finland*
[2]*Department of Computer Science, Aalto University, Finland*
E-mail: masoud.naderpour@helsinki.fi; tommi.meskanen@helsinki.fi; valtteri.niemi@helsinki.fi; andrew.paverd@ieee.org

Received 15 September 2017;
Accepted 8 November 2017

Abstract

Intelligent transportation systems are on their way toward wide deployment. Vehicle to everything (V2X) communication, as an enabler for safer and more convenient transportation, has attracted growing attention from industry and academia. However, security and privacy concerns of such communication must be addressed before it can be widely adopted. In this paper we analyze the security and privacy requirements of V2X communication. Specifically, we focus on lawful identity resolution (i.e., de-anonymization) in V2X communication, and consider recent regulatory changes in this area. Based on this, we define an expanded set of technical requirements for identity resolution in V2X communication. We then propose a solution for the problem statement where the involved parties may be dishonest but not colluding.

Keywords: De-anonymization, Auditability, V2X, Security Credential Management System (SCMS).

1 Introduction

Vehicular networks, and more specifically vehicle to vehicle (V2V) communication, have drawn close attention from the automobile industry and academia for a long time with the aim of increasing vehicles' safety and expanding

Journal of ICT, Vol. 5_1, 91–106.
doi: 10.13052/jicts2245-800X.515

drivers' spatial awareness. Dedicated short range communication (DSRC) has been one of the leading technologies to enable such ad-hoc communications, and standardization bodies in the US and Europe have already developed mature standards (e.g., IEEE 1609 [1] and ETSI ITS G5 [6]). Vehicle to everything (V2X) communication, which comprises inter-vehicle communication and vehicle to road infrastructure, pedestrians, and network, has been promoted as one the fundamental enablers, which goes beyond the safety applications, to support cooperative intelligent transportation systems.

5G communication networks, with their ambitious goals of pervasive connectivity and a versatile and adaptable infrastructure for many verticals and businesses, are one of the most promising candidates to enable V2X services. Indeed, V2X is a key vertical for the upcoming generation of mobile networks, and recently some early standards have been completed by the 3GPP on enhancing the LTE architecture for V2X communications [2, 4].

In the V2X ecosystem, vehicles frequently disseminate safety and warning messages to neighboring vehicles in order to increase safety, facilitate cooperative driving, and improve the overall efficiency of transportation. These messages include information such as vehicle position, speed, and heading. Despite all the benefits they bring, a malicious user might use these messages to gain some advantages over other vehicles or even worse, to cause traffic disruptions, car crashes, or even fatal injuries. To avoid abuse or malicious attacks, the messages must be sent from authorized vehicles and their authenticity and integrity must be verified at destination. However, this raises serious concerns toward vehicle privacy. Any eavesdropper can record and analyze the messages, and and use any unique identifiers in the messages to track the vehicles. This has motivated the need for privacy in V2X communication.

Nevertheless, to hold the participating vehicles in the system accountable and to facilitate authorized law enforcement activities, privacy cannot be an absolute requirement, and must be conditional in the context of V2X. In case of a dispute or investigation, law enforcement may need to have the ability to *de-anonymize* the sender of a message, or to track its movements. This is referred to as *identity resolution*.

Although identity resolution itself has been addressed in various research projects and privacy-preserving solutions for V2X communications, e.g., [7, 9, 14], the interplay between the technical and legal aspects of this mechanism have not been previously considered. For instance, Switzerland recently passed a law that enforces the transparency of law enforcement actions toward citizens surveillance. If a surveillance operation has taken place, but

no further action is taken, the relevant authorities are obligated to inform the subject(s) about the operation within one month after the end of the operation [15].

2 Requirements in V2X

Location tracking is one of the main privacy concerns in V2X communication and it has been studied extensively in various research projects. In this section, we briefly discuss the main security and privacy requirements in V2X communication with regard to the exchanged messages. *Authenticity, integrity,* and *confidentiality* are typically listed as critical security requirements for the correct functioning of the system and to enable V2X value-added services. However, to protect the location privacy of the vehicles, the messages must not have any identifiable information towards the vehicle, which may cause tension with the authenticity requirement. Furthermore, it should not be possible for the adversary to link together multiple messages from the same vehicle, except for a short period to allow correct functioning of the safety applications, as this could allow the adversary to build up a location profile for the vehicle, from which the owner/driver could possibly be identified (e.g., based on a residential address). Thus, *anonymity* and *unlinkability* are the fundamental privacy requirements to prevent location tracking. In this regard, the 3GPP specifications consider using specific identifiers for V2X communication while taking anonymity requirements into account [3].

Having defined the security and privacy requirements from the users' perspective, we now consider requirements from the perspective of law enforcement agencies (LEAs). We argue that it is critical to consider such requirements to ensure that research efforts are compatible with real-world regulatory constraints, and ultimately to improve *deployability*. It is likely that real-world deployments will have to provide *lawful interception* capabilities, which enable authorized LEAs to remove the confidentiality protection on messages. The lawful interception requirements from the 3GPP are described in [5]. Furthermore, LEAs may require the ability to *de-anonymize* the real identity of a specific vehicle's owner/user, based on captured messages. We envisage that the de-anonymization could occur in two levels: i) in the weaker form, it is possible to link together messages sent from the same vehicle, thus constructing a (partial) location profile without directly linking this to a real identity; and ii) the stronger form in which the real identity of the vehicle is immediately resolved. Either way, as discussed in Section 1, we require all de-anonymizations to be authorized by a competent authority. On the other

hand, V2X users must eventually be able to audit if they have been subject of any de-anonymization.

3 Pseudonymity Schemes

Various pseudonymity schemes have been introduced to provide anonymity and unlinkability [13]. Among the proposed solutions, a large subset relies on digital certificates and deployment of a public key infrastructure (PKI) for vehicular communications, e.g., [8, 10, 16]. Figure 1 presents a basic overview of the PKI-oriented pseudonymity schemes and the primary entities involved: the *long-term certificate authority* (LTCA), also known as enrollment authority, and the *pseudonym certificate authority* (PCA). After registration, vehicles receive a long-term certificate from the LTCA, and can later use this certificate to obtain short-term certificates, which are used as *pseudonyms*.

In this section, we discuss the *Security Credential Management System* (SCMS) [11, 12, 16], a leading candidate for standardization in the USA. In Section 4, we explain how our proposed solution can be built upon SCMS. Compared to the basic architecture in Figure 1, the main enhancements of SCMS are that it makes the system more resilient against insider attackers in back-end authorities, and that it reduces the size of the certificate revocation lists (CRLs). We briefly introduce the main components in the SCMS architecture as shown in Figure 2, and describe how pseudonym certificates are obtained by vehicles such that no single authority can track vehicles.

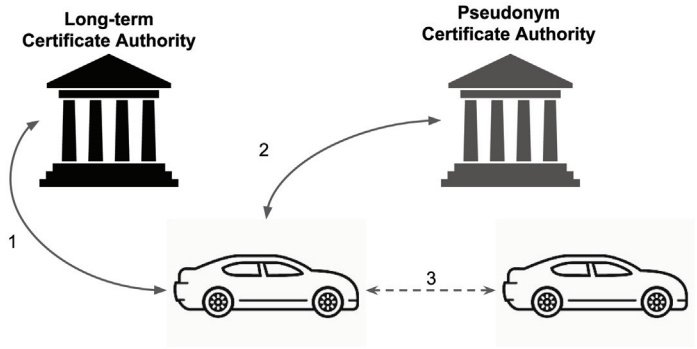

Figure 1 Generic PKI-oriented pseudonymity scheme, 1. Vehicle registers to the V2X system by obtaining a *long-term certificate;* 2. Using its long-term certificate, the vehicle can request *pseudonym certificates;* 3. The vehicle can communicate with other vehicles using pseudonyms to protect privacy.

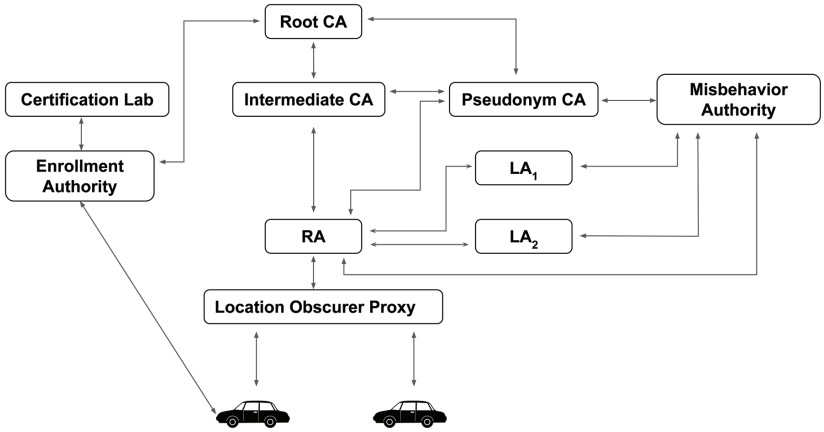

Figure 2 Simplified architecture of *Security Credential Management System* (SCMS) [16].

SCMS introduces a new authority, called the *registration authority* (RA), as an anonymizer proxy between the vehicle and PCA. Similarly to the basic architecture, the vehicle registers with SCMS by enrolling at the enrollment authority and obtaining a long-term *enrollment certificate.*

Once this registration procedure is complete, the vehicle can request pseudonyms. Figure 3 summarizes the sequence of messages involved in pseudonym provisioning. The vehicle first creates the pseudonym certificates request, signs it with the enrolment certificate, encrypts the signed request for the RA and sends it to the RA ①. The RA merges the certificate request information with the linkage information from the linkage authorities (LA_1, LA_2) to create a series of individual certificate requests. It also stores the mapping between these certificates requests and the enrolment certificates. The RA accumulates requests from different vehicles, shuffles them for privacy reasons and sends them to the PCA ②. The PCA signs the pseudonym certificates, encrypts them with a vehicle-specific key, signs the encrypted versions, and returns the encrypted and signed pseudonym certificates to the RA ③. The PCA stores the information about binding between the individual requests and the issued pseudonym certificates. The RA makes the pseudonym certificates available for download to the vehicle ④.

In case of a misbehaving or a faulty vehicle in the system, there are two *linkage authorities* (LA_1, LA_2) that release two linkage seeds which then are added to a regularly-published certificate revocation list (CRL). Using this list, other vehicles can detect pseudonyms from the revoked vehicles, thus preventing the revoked vehicles from participating in the V2X communication.

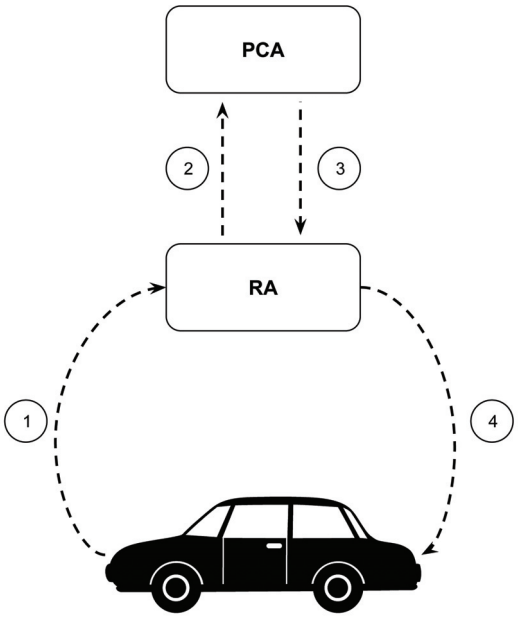

Figure 3 Sequence of messages in SCMS pseudonym provisioning.

The revocation mechanism is initiated and coordinated by the *Misbehaviour authority* (MA). Note that no single authority in the SCMS architecture is able to de-anonymize or link the pseudonyms of a vehicle independently. Nevertheless, MA has been designed with access to the necessary protocols and interfaces to other authorities to coordinate such collaborations leading to the revocation of the pseudonyms of a specific vehicle. With minimal changes, it is possible to enhance SCMS so that the MA could also initiate a de-anonymization operation. At the end of de-anonymization operation, the MA receives the enrolment certificate (in encrypted form) of the de-anonymized vehicle from the RA. In Section 4, we assume that de-anonymization operations are already available in SCMS, and build our proposed solution for *auditable* de-anonymization on top of the SCMS design.

SCMS also leverages other cryptographic methods in order to increase the overall efficiency of the system, e.g., in terms of communication complexity and communication rounds. For instance, it is possible for a vehicle to request a set of pseudonyms with a single request and public key. Other functionality provided by SCMS is beyond the scope of this paper.

4 Proposed Solution

We leverage the pseudonymity scheme of SCMS presented in the previous section, and propose an *auditable de-anonymization* capability for this scheme. The following entities are involved in a de-anonymization scenario:

- **Law enforcement agency (LEA)**: the LEA may need to de-anonymize certain V2X messages, which it has previously recorded. For simplicity we refer to the LEA as the *police*.
- **Identity resolution authority**: we assume that all identity resolutions are authorized by a court order. We refer to the identity resolution authority as the *judge*.
- **Vehicle owner**: A vehicle owner in this context is the entity who wants to check if his/her vehicle has been de-anonymized. The vehicle owner is therefore the *enquirer*.[1]

We propose our solution in the context of two different schemes: The first scheme considers the current design of SCMS and can be deployed with minimal changes to SCMS. The most significant change is that it requires a bidirectional interface between the RA and the MA, which was previously a one-way channel from the MA to the RA, as depicted in Figure 4.

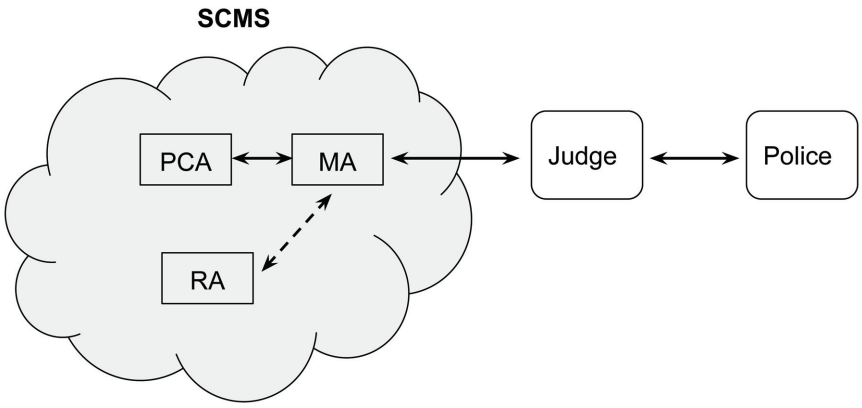

Figure 4 The entities involved in a de-anonymization operation and the interactions between the entities.

[1]In this paper we consider only the case in which the vehicle owner is the enquirer, but our requirements and scheme could be adapted such that other entities (e.g., civil rights groups) could also perform some of the functionality of the enquirer on behalf of the public.

Although this proposal is already deployable, it has some shortcomings, e.g., it may be possible to entities other than the vehicle owner to detect when a vehicle has been under surveillance. The second scheme introduces a new secret key which is shared between SCMS and the owner. This increases the security and privacy level of the solution and also takes into account possible ownership changes of the vehicle.

4.1 First Scheme

In this scheme, both the police and the judge are external entities from the SCMS perspective, as shown in in Figure 4. A de-anonymization task starts when the police send a pseudonym to the judge. The judge, as the identity resolution authority, works jointly with SCMS to recover the identity of the pseudonym. First, the judge sends the pseudonym together with explicit authorization for de-anonymization to the MA. Inside the SCMS, the MA coordinates between the PCA and RA such that the RA recovers the enrollment certificate of the vehicle. The RA encrypts the enrollment certificate with a (potentially) long-term public key of the police. Then it sends the encrypted enrollment certificate to the judge via the MA. Since the judge might be a dishonest entity who wishes to de-anonymize innocent vehicles, the MA and the police should continuously monitor that judge follows this protocol. At the end of this section, we present a proposal for how this monitoring could be performed.

Note that in the current design of SCMS, the only component that is inspected before issuing an enrollment certificate is the vehicle's on-board unit (OBU). This essentially means that when a vehicle requests new pseudonyms, the RA just inspects if the embedded OBU is a certified device. Thus, no identifiable information about the vehicle itself is included in the certificate that comes with the request. Therefore, we assume that the police are able to map enrollment certificates to the identity of the vehicle's owner (e.g., using information from a vehicle licensing authority).

The idea behind the solution is simple yet effective. We use a chain of logs which is integrity protected by a hash chain to record all the de-anonymization transactions. The judge is obligated to release regular increments to the *logchain*.[2] The logchain is *readable* by anybody but only *writeable* by the judge. The following fields are included in the log:

[2]Alternatively, this could be a public *blockchain*.

- **Search tag:** The search tag has the following format:

$$tag = \left[T, \left\langle [enroll\_cert]_{PK_p}, pseudo \right\rangle_{PK_i}\right]$$

  where *T* is a time interval and $\langle [enroll\_cert]_{PK_p}, pseudo\rangle_{PK_i}$ is the encryption of the enrollment certificate (encrypted using the public key PK_p and one of the pseudonyms allocated to the vehicle for the interval T, using the public key PK_i. Both public keys PK_p and PK_i belong to the police. We discuss key distribution and use later in this section.
- **Time-stamp**: The judge is obligated to include a time-stamp indicating the time at which the log entry was created. As the chain is extended, this eliminates the risk that the judge could retroactively insert log entries for earlier points in time.
- **Data**: The judge encrypts all additional information related to a de-anonymization request using the public key PK_i provided by the police.
- Link to the previous log entry: Each log entry includes the hash value of the previous log entry, ensuring that new entries cannot be added in the middle of the logchain.

Periodically (e.g., daily), the police generate a key pair (PK_i, sk_i) for a *deterministic* public key encryption scheme (e.g., the RSA cryptosystem), and send the public key PK_i to the judge *privately*. The judge uses this key to encrypt the specified fields in the log. This public key PK_i is also delivered to the MA when the judge makes a de-anonymization request. The MA needs this public key to monitor that the judge adds correct logs to the logchain. The RA does not get PK_i but instead uses a separate long-term public key PK_p of the police to encrypt the enrollment certificate. The police make this public key PK_p (also for a deterministic cryptosystem) available to the public, including vehicle owners and the RA. With the knowledge of PK_i, the encrypted enrollment certificate, and the pseudonym, the MA can verify that the judge adds a correct log entry to the logchain. Note that these additional steps do not change the security and privacy guarantees of SCMS: neither the MA nor the RA is able to link pseudonyms to enrollment certificates.

In order to fulfil the new auditability requirements defined in Section 2, the judge will release each public key PK_i after a certain period of time. After PK_i is released, vehicle owners can ascertain whether they have been de-anonymized by checking the elements of the logchain. Note that in SCMS,

each vehicle has multiple valid pseudonyms at any given time (e.g., 20 pseudonyms per week), and frequently switches between these pseudonyms in order to avoid location tracking attacks. For each log entry, the enquirer fetches all pseudonyms it used during the interval *T* specified in the search tag. He then encrypts the vehicle's enrollment certificate with the public key used by the police PK_p, concatenates this with each possible pseudonym, and encrypts this using the public key PK_i associated with the log to produce $\langle [enroll\_cert]_{PK_p}, pseudo \rangle$. This is then compared to the corresponding term in the log entry. Since all the encryption operations are deterministic, the enquirer will find a match if his pseudonym has been de-anonymized. If a match is found, the enquirer can request further information from the judge about the de-anonymization operation (e.g., by requesting decryption of the data field in the log entry).

4.1.1 Security analysis

We now analyse the security of our approach. We assume that the police, judge, MA, and RA will not collude, and that all entities can authenticate each other correctly. In particular, we are concerned with possible deviations from the protocol (e.g., unauthorized de-anonymization, or de-anonymization without auditability). Neither the police nor the RA can start an unauthorized de-anonymization without authorization from the judge (enforced by the MA). The judge cannot initiate unauthorized de-anonymization because both the MA and the police monitor the logchain, and either the police will notice an extra log entry, or the MA will notice a missing entry. Moreover, deletion of log entries is not possible without detection by the public, due to the properties of the hash chain. Only the MA is able to initiate an unauthorized de-anonymization request, however in this case the MA would only get an encrypted enrollment certificate. Even when authorized de-anonymization takes place, the police are the only entity that learn both a vehicle's pseudonym and enrollment certificate. In principle, a dishonest entity could leak this information, but this is beyond the scope of this paper.

4.1.2 Limitations

The above idea of using the same public key for all the logs that have been generated within the same time period (e.g., on a daily basis) might not be sufficiently flexible to address the legal requirements. For example, as explained in Section 1, Swiss legislation obligates informing the subject of surveillance within one month after the conclusion of the investigation. Since each investigation may require a different amount of time, this would either

result in some subjects being informed late (if at all), or leaking details of ongoing investigations. One possible approach is for the police to send a unique key to the judge for every request, so that each de-anonymization can be revealed individually after the investigation has been completed. However, in this case, the police and the MA must be especially vigilant in ensuring that every entry is added to the logchain, since this can no longer be verified by the public.

As explained in Section 3, a vehicle can authenticate itself to the RA using its long-term enrollment certificate. Specifically, the vehicle uses the private key corresponding to its enrollment certificate to sign an authentication challenge (as usual), and sends its enrollment certificate to the RA. However, in our scheme, when an enquirer checks the log for entries related to his vehicle, he uses the enrollment certificate as a type of authentication token (i.e., the enquirer encrypts the enrollment certificate itself, without using the corresponding private key). This non-standard use of the certificate is necessary in our design, because the RA only has access to the enrollment certificate, not the corresponding private key. The consequence is that if an attacker somehow obtains both the vehicle's pseudonym and enrollment certificate (even without the private key), the attacker can check whether the vehicle has been de-anonymized.

In the current SCMS specification, a vehicle's enrollment certificate is considered to be a long-term certificate that is issued with a validity period of 30 years (i.e., generally for the lifetime of the vehicle). Thus the enrollment certificate remains the same even if the ownership of the vehicle changes. This means that previous owners may still have access to the enrollment certificate even after handing over the vehicle, and could check whether the vehicle's new owner has been de-anonymized.

4.2 Second Scheme

To overcome some of the limitations of the first scheme, we introduce a secret key, called the *private audit key* (PAK), that is shared only between the RA and the current owner of the vehicle. The RA maintains (or has access to) a database of mappings between enrollment certificates unique PAKs. When vehicle ownership changes, the new owner registers a new PAK.

The details of this scheme are very similar to the first scheme. The judge authorizes the de-anonymization operation and sends the pseudonym to the MA. The MA initiates the de-anonymization and coordinates between the PCA and RA. The RA recovers the enrollment certificate and returns the

encryption of the enrollment certificate and the corresponding PAK to the MA. The judge creates a log entry as in the first scheme except that the search tag now includes the PAK, in addition to the enrollment certificate and the pseudonym: $[T, \langle [PAK, enroll\_cert]_{PK_p}, pseudo \rangle_{PK_i}]$. Note that the PAK should have sufficient entropy to prevent a brute-force attack. Moreover, the MA and the police continuously monitor the judge to ensure that the log entries include the correct information and are added to the logchain immediately. The judge releases the public keys PK_i from the police periodically after checking that the operation has been completed. Using these public keys, enquirers can verify whether their vehicles have been de-anonymized, as explained in the first scheme.

The addition of the owner-specific PAK prevents past owners from auditing future de-anonymizations. Furthermore, even if the adversary manages to learn both a vehicle's pseudonym and enrollment certificate, he cannot audit de-anonymizations without knowing the PAK.

4.3 Discussion on Roles

It might be desirable to merge the functionality of one or even both external entities (i.e., the police and the judge) into the SCMS architecture. In the following, we show why such merging would diminish the security guarantees of the system.

- **Merging the police and RA**: even though the judge is still an independent entity, merging the police and RA would give this new entity the possibility to send falsified data as the encryption of the enrollment certificate (and the PAK) to the MA, which is then included in the logchain. For example, not including the correct enrollment certificate (and PAK) in the log would prevent the vehicle owner from auditing possible de-anonymization events.
- **Merging the police and MA**: Merging these two entities would allow unauthorized de-anonymization, since the MA is usually responsible for checking the authorization from the judge. After obtaining authorization from the judge for one pseudonym, this entity could change the pseudonym before sending it to the PCA, since the RA is unable the check the pseudonym for which de-anonymization has been authorized.
- **Merging the judge with the RA**: In this case, the judge would learn both the pseudonym and enrollment certificate, which is undesirable.
- **Merging the judge with the MA**: the police would not notice if this new entity initiates a de-anonymization operation and does not create an entry

in the logchain. This type of architecture could potentially still be feasible if the RA checks immediately that an item is added to the logchain and the police check that there is a log entry for every de-anonymization request.

In summary, it is not feasible to merge the external entities with any of the pre-existing SCMS entities without diminishing the security guarantees of the system.

5 Conclusion

The standardization of V2X communications in 5G is yet to be completed. Nevertheless, security and privacy requirements must be taken into account from the very beginning. In this paper, we briefly discussed the security and privacy requirements in V2X communications. Particularly, we defined a new requirement, *auditable de-anonymization*, for pseudonymity schemes which in which identity resolution is possible. We believe that such requirement will be necessary in real-world deployments, in order to comply with regulation. We present two schemes to provide auditable de-anonymization capabilities on top of existing PKI-based pseudonym schemes.

Acknowledgement

We thank N. Asokan, Filippo Bonazzi, and Moreno Ambrosin for contributing to the formulation of the target scenario and privacy requirements. This work has been supported by an Intel research grant.

References

[1] IEEE guide for wireless access in vehicular environments (WAVE) – architecture. IEEE. doi:10.1109/IEEESTD.2014.6755433

[2] 3GPP. (2015). Study on LTE support for Vehicle-to-Everything (V2X) servicese. Release 14. Available at: http://www.3gpp.org/ftp/Specs/archive/22_series/22.885/

[3] 3GPP. (2016). Architecture enhancements for V2X services. Release 14. Available at: http://www.3gpp.org/ftp/Specs/archive/23_series/23.285/

[4] 3GPP. (2016). Study on enhancement of 3GPP support for 5G V2X services. Release 15. Available at: http://www.3gpp.org/ftp/Specs/archive/22_series/22.886/

[5] 3GPP. (2017). 3G security; Lawful interception requirements. Release 14. Available at: http://www.3gpp.org/ftp/Specs/archive/33_series/33.106/

[6] ETSI ES 202 663. (2009). European profile standard for the physical and medium access control layer of Intelligent Transport Systems operating in the 5 GHz frequency band. *ETSI Final draft ETSI ES 202 663 V1.1.0.*

[7] Bißmeyer, N., Petit, J., and Bayarou, K. M. (2013). CoPRA: Conditional pseudonym resolution algorithm in VANETs. In *Wireless On-demand Network Systems and Services (WONS), 2013 10th Annual Conference,* 9–16. IEEE.

[8] Bißmeyer, N., Stübing, H., Schoch, E., Götz, S., Stotz, J. P., and Lonc, B. (2011). A generic public key infrastructure for securing car-to-x communication. In *18th ITS World Congress, Orlando, USA,* 14.

[9] Fischer, L., Aijaz, A., Eckert, C., and Vogt, D. (2006). Secure Revocable Anonymous Authenticated Inter-vehicle Communication (SRAAC). In *4th Conference on Embedded Security in Cars (ESCAR 2006), Berlin, Germany*.

[10] Khodaei, M., Jin, H., and Papadimitratos, P. (2014). Towards deploying a scalable & robust vehicular identity and credential management infrastructure. In *Vehicular Networking Conference (VNC),* 33–40. IEEE.

[11] Crash Avoidance Metrics Partners LLC. (2016). *EE Requirements and Specifications Supporting SCMS Software Release 1.1*. Technical Report. Available at: http://www.its.dot.gov/pilots/pdf/SCMS_POC_EE_Requirements.pdf

[12] Crash Avoidance Metrics Partners LLC. (2016). SCMS proof-of-concept interfaces. Technical report.

[13] Petit, J., Schaub, F., Feiri, M., and Kargl, F. (2015). Pseudonym Schemes in Vehicular Networks: A Survey. In *IEEE communications surveys & tutorials*, 17, 228–255.

[14] Schaub, F., Kargl, F., Ma, Z., and Weber, M. (2010). V-tokens for Conditional Pseudonymity in VANETs. In *Wireless Communications and Networking Conference (WCNC),* 1–6. IEEE.

[15] Titcomb, J., France-Presse, A. (2016). *Switzerland will notify citizens when they have been spied on under new surveillance laws*, (Accessed: May 15, 2017). Available at: http://www.telegraph.co.uk/technology/2016/09/26/switzerland-will-notify-citizens-when-they-have-been-spied-on-un/

[16] Whyte, W., Weimerskirch, A., Kumar, V., and Hehn, T. (2013). A security credential management system for V2V communications. In *Vehicular Networking Conference (VNC),* 1–8. IEEE.

Biographies

Masoud Naderpour is currently working as a doctoral student in University of Helsinki, focusing on the security and privacy aspects of 5G mobile systems and cellular-V2X. He holds a master's degree in information security and cryptography from University of Turku, Finland.

Tommi Meskanen had his PhD in 2005 in mathematics. He used to work in various positions at the Department of Mathematics in University of Turku from 2000 to 2016. During this time he lectured several cryptography courses. Since 2016 he has been working as a senior researcher at the Department of Computer Science in University of Helsinki.

Andrew Paverd is a Research Fellow at Aalto University, Finland, and a Deputy Director of the Helsinki-Aalto Center for Information Security. He received his BSc in Electrical Engineering from the University of the Witwatersrand, Johannesburg, his MSc in Electrical and Computer Engineering from the University of Cape Town, and his DPhil in Computer Science from the University of Oxford. He is a recipient of the 2017–18 Fulbright Cyber Security Scholar Award. His research interests are primarily in the area of systems security and trusted execution environments, and also include the design and analysis of security protocols, distributed consensus mechanisms, and privacy-enhancing technologies.

Valtteri Niemi is a Professor of Computer Science in University of Helsinki and leads the Secure Systems research group. Earlier he has been a Professor of Mathematics in two other Finnish universities: University of Vaasa during 1993–97 and University of Turku during 2012–2015. Between these two academic positions Niemi served for 15 years in various roles at Nokia Research Center and was nominated as a Nokia Fellow in 2009. At Nokia, Dr. Niemi worked for wireless security, including cryptological aspects and privacy-enhancing technologies. He participated 3GPP SA3 (security) standardization group from its beginning and during 2003–2009 he was the chairman of the group. He has published more than 70 scientific articles and he is a co-author of four books and more than 30 patent families.