ETSI TR 103 415 V1.1.1 (2018-04)

Intelligent Transport Systems (ITS);
Security;
Pre-standardization study on pseudonym change management

Reference

DTR/ITS-00527

Keywords

ITS, privacy, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Intelligent Transport Systems (ITS).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present document is structured as follows:

- Introduction of the state-of-the-art on pseudonym change strategies by studying propositions from the literature and current C-ITS pre-deployment projects as well as the position of other standardization bodies.
- Definition of relevant metrics that may be used to quantify the level of safety and privacy provided by the different strategies. The evaluation of the pseudonym change strategies then follows. Note that in the present document the evaluation itself is not available and will be added in the next release. However, the methodology of evaluation is basically described.
- Definition of an exhaustive list of parameters that are related to pseudonym lifecycle. When available, those definitions come with implementation-specific concrete values springing from pre-deployment projects.
- Guidance and recommendations for future versions of related ETSI specifications.

1 Scope

The purpose of the present document is to realize a pre-standardization study on pseudonyms management for C-ITS in order to provide guidance and recommendations for the future versions of related ETSI ITS specifications.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] J. Petit, F. Schaub, F. Kargl: "Pseudonym schemes in vehicular networks: a survey", ACM Computing Surveys, August 2014.

[i.2] D. Eckhoff, C. Sommer, T. Gansen, R. German, F. Dressler: "Strong and affordable location privacy in VANETs: identity diffusion using time-slots and swapping", IEEE Vehicular Networking Conference (VNC'10), 2010.

[i.3] PRESERVE project Technical Report 2: "V2X Privacy Protection Position Statement", 2012.

[i.4] PRESERVE project deliverable D5.3: "Deployment issues report v3", 2013.

NOTE: Available at https://www.preserve-project.eu/deliverables.

[i.5] S. Lefèvre, J. Petit, R. Bajcsy, C. Laugier, F. Kargl: "Impact of V2X Privacy Strategies on Intersection Collision Avoidance Systems", IEEE Vehicular Networking Conference (VNC'13), 2013.

[i.6] A. Pfitzmann, M. Hansen: "Anonymity, unobservability, and pseudonymity: a proposal for terminology", Designing Privacy Enhancing Technologies, 2000.

[i.7] A. Serjantov, G. Danezis: "Towards an information theoretic metric for anonymity", Designing Privacy Enhancing Technologies, 2002.

[i.8] C. Diaz, S. Seys, J. Claessens, B. Preneel: "Towards measuring anonymity", Designing Privacy Enhancing Technologies, 2002.

[i.9] J. Yin, T. Elbatt, G. Yeung, B. Ryu, S. Habermas, H. Krishnan, T. Talty: "Performance evaluation of safety applications over DSRC vehicular ad hoc networks", VANET'04: Proceedings of the 1st ACM International Workshop on Vehicular Ad hoc Network, 2004.

[i.10] S. Yousefi, M. Fathy: "Metrics for performance evaluation of safety applications in vehicular ad hoc networks", Transport, 2008.

[i.11] G. Korkmaz, E. Ekici, F. Özgüner, Ü. Özgüner: "Urban multi-hop broadcast protocol for inter-vehicle communication systems", VANET'04: Proceedings of the 1st ACM International Workshop on Vehicular Ad hoc Network, 2004.

[i.12] Q. Xu, T. Mak, J. Ko, R. Sengupta: "Vehicle-to-vehicle safety messaging in DSRC", VANET'04: Proceedings of the 1st ACM International Workshop on Vehicular Ad hoc Network, 2004.

[i.13] J. Freudiger, M.H. Manshaei, J.-P. Hubaux, D.C. Parkes: "On non-cooperative location privacy: a game-theoretic analysis", CCS'09: Proceedings of the 16th ACM conference on Computer and Communications Security, 2009.

[i.14] J. Freudiger, M. Raya, M. Felegyhazi, P. Papadimitratos, J.-P. Hubaux: "Mix-zones for location privacy in vehicular networks", WiN-ITS'07: ACM Workshop on Wireless Networking for Intelligent Transportation Systems, 2007.

[i.15] A.R. Beresford, F. Stajano: "Location Privacy in Pervasive Computing", Journal IEEE Pervasive Computing, 2003.

[i.16] ETSI TS 101 539-1 (V1.1.1) (08-2013): "Intelligent Transport Systems (ITS); V2X Applications; Part 1: Road Hazard Signalling (RHS) application requirements specification".

[i.17] R. K. Schmidt, R. Lasowski, T. Leinmüller, C. Linnhoff-Popien, G. Schäfer: "An approach for selective beacon forwarding to improve cooperative awareness", Vehicular Networking Conference (VNC), 2010.

[i.18] C2C-CC: PKI Memo V 1.7: "C2C-CC public key infrastructure memo," CAR 2 CAR Communication Consortium, Tech. Rep., February 2011.

[i.19] C2C-CC Basic System Profile version 1.1.0, dated 21.12.2015.

[i.20] Eric R. Verheul: "Issue First Activate Later Certificates for V2X- Combining ITS efficiency with privacy".

NOTE: Available at https://eprint.iacr.org/2016/1158.pdf.

[i.21] Bai F, Krishnan H.: "Reliability Analysis of DSRC Wireless Communication for Vehicle Safety Applications". Proc 2006 IEEE Intell Transp Syst Conf. 2006;355-62.

[i.22] ETSI TS 103 097: "Intelligent Transport Systems (ITS); Security; Security header and certificate formats".

[i.23] ETSI TS 102 940: "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management".

[i.24] ETSI EN 302 637-2: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service".

[i.25] ETSI EN 302 637-3: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service".

[i.26] ETSI TS 102 941: "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management".

[i.27] ETSI TS 102 723-8: "Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 8: Interface between security entity and network and transport layer".

[i.28] ETSI TS 102 636-6-1: "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols".

[i.29] ETSI TR 102 893: "Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)".

[i.30] ETSI TS 101 539-3 (V1.1.1) (11-2013) "Intelligent Transport Systems (ITS); V2X Applications; Part 3: Longitudinal Collision Risk Warning (LCRW) application requirements specification".

[i.31] SAE J2945/1: "On-board System Requirements for V2V Safety Communications".

[i.32] "Deutsches Zentrum für Luft- und Raumfahrt" (German Aeronautics and Space Research Center - DLR).

[i.33] ETSI TS 101 539-2: "Intelligent Transport System (ITS); V2X Applications; Intersection Collision Risk Warning (ICRW) application requirements specification".

[i.34] NHTSA: "Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application", August 2014.

[i.35] C-ITS Platform - Year1 Report - WG1 Annex 2 Cost-Benefits analysis Summary Report.

NOTE: Available at https://ec.europa.eu/transport/themes/its/c-its_en.

[i.36] Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), Release 1, December 2017.

NOTE: Available at https://ec.europa.eu/transport/sites/transport/files/c-its_security_policy_release_1.pdf.

[i.37] Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), Release 1, June 2017.

NOTE: Available at https://ec.europa.eu/transport/sites/transport/files/c-its_certificate_policy_release_1.pdf.

[i.38] SAE J2735: "Dedicated Short Range Communications (DSRC) Message Set Dictionary™".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TS 102 940 [i.23], ETSI TS 102 941 [i.26], ETSI TR 102 893 [i.29] and the following apply:

attacker: one or more collaborative nodes that exploit the system in order to get benefits or to disrupt it

tracking: action of rebuilding the path of an ITS-S based on the information it provides in its V2X messages

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 102 940 [i.23], ETSI TS 102 941 [i.26], ETSI TR 102 893 [i.29] and the following apply:

ADAS	Advanced Driver-Assistance Systems
AID	Application ID
AID-SSP	AID Service Specific Permissions
AT	Authorization Ticket
BSP	Basic System Profile (C2C-CC document)
C2C-CC	Car-2-Car Communication Consortium
CAPEX	Capital Expenditure
C-ITS	Cooperative ITS
CTL	Certificate Trust List
EC	Enrolment Credential
ID	Identifier
IFAL	Issue First, Activate Later (certificate issuance process design)
ITS-G5	802.11p radio access technology in the 5,9 GHz band
KPI	Key Performance Indicator
OBU	On-Board Unit
OPEX	Operational Expenditure
RCA	Root Certificate Authority
RHS	Road Hazard Signalling
SDO	Standards Developing Organization

SN-SAP	Security/Network Service Access Point
SSP	Service Specific Permission
TCO	Total Cost of Ownership
V2X	Vehicle-to-any communication

4 Pseudonym change strategies

4.1 Existing approaches in the literature

4.1.1 Overview

Many research works on pseudonym change strategies have been conducted over the last years. In [i.1] authors present an interesting and exhaustive survey that depicts the current status of this topic.

The clauses below describe the strategies identified in the literature. For more details about a specific strategy, refer to the references indicated in the strategy description.

4.1.2 Fixed parameters

One of the easiest strategy to implement consists of defining a fixed pseudonym change parameter. Many parameters can be considered such as time (e.g. change pseudonym each 5 minutes), number of V2X signed messages (e.g. change pseudonym each 100 messages) or distance (e.g. change pseudonym each 500 m).

The main drawback of such strategy remains in its simplicity. It is indeed quite easy for an eavesdropping attacker to determine the parameter value of a specific vehicle, making tracking of this vehicle trivial.

Also note that a combination of several parameters can be considered. For instance, a strategy may define that pseudonym is changed every 10 minutes or 1 000 m, whichever condition is met first.

4.1.3 Randomness

In order to cope with the predictability of the previous strategy, randomness can be inserted. The pseudonym is still changed according to a fixed parameter to which a random value is added. For instance, a pseudonym can be changed after 5 minutes of use plus or minus 1 minute, after moving 1 000 m plus or minus 200 m, etc.

The addition of a random factor helps to prevent attackers for determining the pseudonym change periodicity. However, the linkage of pseudonyms remains possible and trivial if only a few vehicles change pseudonym because the other vehicles keep the same one. Also, an attacker can easily track vehicles that have changed pseudonym by using some trajectory predictability algorithms such as Kalman filters.

4.1.4 Silent period

This strategy proposes that vehicles remain silent (i.e. do not send any V2X message but still process incoming messages) during a certain amount of time after they changed their pseudonym. Tracking thus becomes much more difficult especially when vehicles change pseudonym on situations where the computation of the predicted trajectory is more complex like at road intersections. However, the drawback of this strategy is that it also affects the safety level as vehicle are not allowed to send safety messages during the silent period.

4.1.5 Vehicle-centric

In this strategy vehicles independently change their active pseudonym based on their mobility criteria such as speed or direction. After a pseudonym change, the vehicle enters in a silent period. As a result, tracking become more difficult because the predictability of the vehicle movement is no longer usable. The duration of the silent period may also be determined based on the vehicle mobility.

4.1.6 Density-based

This strategy allows vehicles to change pseudonym only when the neighbouring environment is dense enough, i.e. when a sufficiently large number of neighbouring vehicle are present. That avoids useless pseudonym changes like, for instance, when a vehicle is alone on the road. In such situation it is indeed obvious that pseudonym linkage becomes an easy task.

4.1.7 Mix-zones

4.1.7.1 General

The concept of mix-zone has been first proposed by authors of [i.15]. Generally speaking a mix-zone is a delimited geographical area where no location aware applications are running, i.e. no location aware messages are exchanged between nodes. This creates an area where all nodes within it are "mixed" such that it becomes very difficult for a tracker to determine where and when the node he is currently tracking will leave the mix-zone.

The mix-zone concept has been proposed as a privacy enhancing technique for pseudonym change strategies in C-ITS. Examples of such strategies are presented in the clauses below.

4.1.7.2 Mix-zones at RSU

Several works propose to create mix-zones on strategic places where many vehicles are present like intersections or parking: the higher the density of vehicles, the more efficient the mix-zone is against tracking.

4.1.7.3 Collaborative change

With this strategy, vehicles change pseudonym simultaneously with their neighbours. To this end, vehicles first broadcast messages to advertise each other that they are ready to change. This creates a context-based mix-zone where vehicles do not send location aware messages until they all changed their pseudonym. This synchronous change makes tracking much more complex as all vehicles leave the mix-zone with a new pseudonym. The main drawback of this strategy is that it is less efficient in low density situations.

4.1.7.4 Cryptographic mix-zones

This strategy relies on the use of symmetric key to exchange safety message within a mix-zone. The mix-zone is usually bound to the radio coverage of a RSU. Using traditional asymmetric cryptography, the RSU provides a symmetric key to all vehicles present in the mix-zone. They then use this key to encrypt safety messages [i.14].

4.1.8 Pseudonym swap

In [i.2] authors propose to swap pseudonyms between vehicles. Basically speaking, two vehicles that are close to each other and follow the same trajectory can swap one pseudonym of their respective pool. The protocol includes randomness such that an attacker that tracks one of those vehicle is not able to determine if both vehicles actually swapped a pseudonym and if yes, which one (it can be the one currently in use or another one that will be used later).

Despite this proposal increases well location privacy, it has two main drawbacks which probably makes it unusable (at least in its current form) with ETSI TS 103 097 [i.22] certificates:

1) It becomes very difficult, even impossible, to reveal the link between a pseudonym and the real identity of an ITS-S if required by law enforcement.

2) There is an SSP compatibility issue: vehicles with different SSP will not exchange pseudonym (e.g. a personal vehicle that swaps pseudonym with a police vehicle).

4.2 C-ITS proposed approaches for pseudonym change

4.2.1 Pseudonym change in the PRESERVE project

The PRESERVE project evaluated the impact of privacy (i.e. pseudonym change) on an intersection collision avoidance system [i.4] and [i.5]. They evaluated the pseudonym change strategy recommended by the SAE J2735 [i.38] - pseudonyms are changed every 120 s followed by a random silent period duration comprise between 3 and 13 s.

Results show that the SAE J 2735 [i.38] recommendation provides a decent privacy but drastically decreases safety. This is due to the fact that this recommendation does not consider the state of the environment before changing pseudonym: a vehicle that changes pseudonym while entering a dangerous area will not be visible by other vehicles because of the silent period. To cope with this issue, they propose to take into consideration the environment in which the vehicle progresses before allowing it to change pseudonym. Therefore, a vehicle entering the intersection will not change pseudonym until it leaves this dangerous area. Those results have been conducted by simulation.

From an implementation point of view, the embedded security stack developed in PRESERVE project implements the pseudonym change strategies based on time and on number. Both use a fixed value to which is added a random value. The silent periods and the environment awareness as explained above have not been implemented. They conduct the following conformance and validation tests with the implementation:

- Pseudonym change: the ITS-S changes its pseudonym. The change of all ITS identifiers of the communication stack has not been tested.
- Interoperability: a receiving ITS-S successfully verifies the signature of messages coming from an ITS-S that changed its pseudonym.

The PRESERVE project also expounds in a technical report [i.3] its position statement regarding privacy protection in V2X. They conclude that C-ITS indeed process personal data and thus there is a need for privacy protection. Pseudonym change strategies is an answer to this issue but should be considered as a Best Available Technique.

4.2.2 Pseudonym change in the SCOOP@F project

SCOOP@F is a Cooperative ITS pilot deployment project intending to connect approximately 3 000 vehicles with 2 000 km of roads and highways in France. The Ministry of Sustainable Development managed this project which involved partners such as local authorities, State services in charge of national road management, automotive industries, automotive suppliers, study centres, universities and research centres, from which Cerema and IFSTTAR. The five tests sites scheduled in this project were the following:

- intercity roads in Ile-de-France;
- Bretagne;
- Paris-Strasbourg highway;
- Bordeaux and its by-pass road; and
- County roads in the Isère "département".

Vehicles exchange with the infrastructures and other connected vehicles some information about their position, speed, obstacles, etc. Roads broadcast about traffic conditions, works, speed limit, accidents, obstacles, etc.

In order to protect the privacy of the road users, a regular change of pseudonym is required. SCOOP@F project proposed a pseudonym storage and change strategy for C-ITS network (see figure 1). The provisioned pseudonym are stored in form of pools for a specific duration (Time Slot: TS) corresponding to their common validity period. In fact, the vehicle selects a new pseudonym from its pool based on a Round-Robin algorithm and so on until the expiration of period of validity of the pseudonym pool. It is noteworthy that thanks to the Round-Robin mechanism, the re-use of a pseudonym is not performed in the same order which prevents any attempt of tracking.