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

TECHNICAL REPORT

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

Copyright Notification

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.

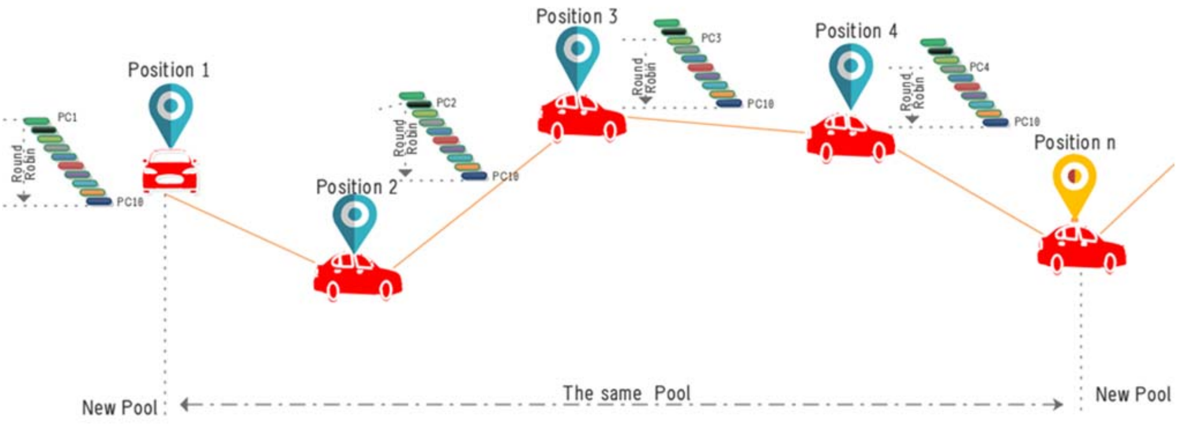

Figure 1: Pseudonym change strategy in SCOOP@F project

The list of parameters for the pseudonym change strategy can be found in clause A.1.

4.2.3 C2C-CC approach to Pseudonym change

4.2.3.1 Pseudonym lifecycle management

Car-2-Car Communication Consortium recommendations regarding the pseudonym lifecycle management are described in [i.18] and [i.19]. They propose several values for the pseudonym lifecycle parameters that are detailed in clause A.2 and included in table 4.

4.2.3.2 Pseudonym change strategy

Recently C2C-CC proposed an innovative pseudonym change strategy in their privacy position paper. The strategy is described below.

The pseudonym change strategy is based on the paradigm that location linking should be avoided whilst enabling road safety applications to function correctly. Therefore it has be chosen as a general rule to separate each trip in at least three unlinkable segments:

- The first segment from the start of a trip, i.e. a location relevant to an individual, to the mid segment.
- The mid segment, where location data are anonymous because they cannot be associated to a location relevant to an individual.
- The last segment that connects the mid segment to the end of the trip, i.e. a location relevant to an individual.

The chosen approach to divide trips in three segments is a goal that in practice cannot be fulfilled for all trips. As a good trade-off between privacy and technical and economic viability it is recommended to define a practical objective: the objective is to trigger pseudonym changes in such a manner that at least 95 % of all trips are correctly divided in three segments. To achieve this objective the following recommended practices are defined:

- A pseudonym change should be triggered at the interruption of a trip which implies the end of a trip and the start of new trip. This condition is established by the following rules: Ignition Off for at least 10 minutes AND Ignition On AND movement detection. This detection is meant to cope with delivery service type of vehicle operation which experience frequent stops during a trip and/or with frequent queues on (urban) motorways and streets.
- The next pseudonym change should be performed during the trip randomly in a range of 800 to 1 500 m from the start position, so to avoid that an eavesdropper can link the first segment of the trip to the second segment by eavesdropping from the same location.
- Further pseudonym changes should be performed at least 800 m from the last pseudonym change (to avoid that an eavesdropper can link subsequent trip segments by eavesdropping from the same location) and within an additional interval of 2 to 6 minutes (to avoid that the same pseudonym can be observed by an attacker at a second location).

NOTE 1: These values have been obtained using traffic statistics in [i.32] and the following example estimations: Statistically 95 % of all trips last longer than 10 minutes or are longer than 3 km.

NOTE 2: A minimum distance of 800 m between pseudonym changes makes sure that the same attacker cannot observe a pseudonym change from the same eavesdropping location assuming the "worst" case RF range of 400 m and the attacker located at the "best" position i.e. 400 m away from the last change and a trip distance corresponding to RF distance.

NOTE 3: A change of pseudonym every 800 m + 2 to 6 minutes give a likelihood to protect against location linking between two eavesdropping locations if the eavesdropping locations are distant at least 2,5 to 6 km in urban environments (vehicle speeds of 50 km/h), or 5 to 14 km in motorway environments (130 km/h).

4.2.4 IFAL Protocol

IFAL [i.20] is a cryptographic protocol for pseudonym certificates that are valid in the future but can only be used together with periodically provided activation codes. IFAL allows for flexible policies, trade-offs between three essential V2X properties: trust, privacy and usability. Pseudonyms can often be changed without a pseudonym ever being reused.

IFAL activation codes are small and can be sent in an SMS, through roadside equipment or even broadcast. Like the Butterfly scheme, IFAL uses key derivation with one base private/public key pair. However in IFAL the security module can be simple as it can be kept oblivious of key derivation.

4.3 Standardization and Policies/legislation framework

4.3.1 SAE approach

SAE provides some recommendations regarding pseudonym change strategies in the SAE J 2945/1 document [i.31]. Basically speaking, they recommend changing pseudonym at startup and then every 5 minutes. They also recommend changing all IDs of the communication stack when changing pseudonym. They recommend as well to lock pseudonym change in critical situations. Details of the parameters provided in [i.31] can be found in clause A.3.

4.3.2 ETSI approach

4.3.2.1 Authorization Tickets

The format of pseudonym is standardized in ETSI TS 103 097 [i.22]. Pseudonym are also referred to as short-term certificates or pseudonym certificates.

V2X Safety messages like CAM [i.24] or DENM [i.25] are cryptographically signed using pseudonym to guarantee that the SENDER's message information is integrity-protected and authentic.

Pseudonyms are public-key certificates which do not include identity information (either vehicle or user identity) and enable to pseudonymize the vehicle/user to prevent location as well as identity tracking.

Privacy is protected by a pseudonym scheme i.e. changing frequently the pseudonym certificates used to authenticate messages such as CAM or DENM.

4.3.2.2 ETSI ITS PKI Design

ETSI security concept uses long-term certificates for identification and accountability of ITS-S, named *Enrolment Certificates* and short-lived, anonymized certificates for V2V/V2I communications, named *Authorization Tickets* or *pseudonym certificates*.

Privacy concerns are introduced due to the content of safety messages (CAM and DENM) and due to the cryptographic signature applied to the messages. Cryptographic certificates allow tracking of vehicles. Users privacy is protected by a pseudonym scheme i.e. changing frequently the pseudonym certificates used to authenticate safety messages. Thereby, the tracking of vehicles is avoided or, at least, made more difficult. To meet this privacy goal, the PKI has to issue and distribute a large set of pseudonym certificates to each ITS-S. The architecture of the ETSI ITS Trust Model is specified in ETSI TS 102 940 [i.23] and presented in figure 2.

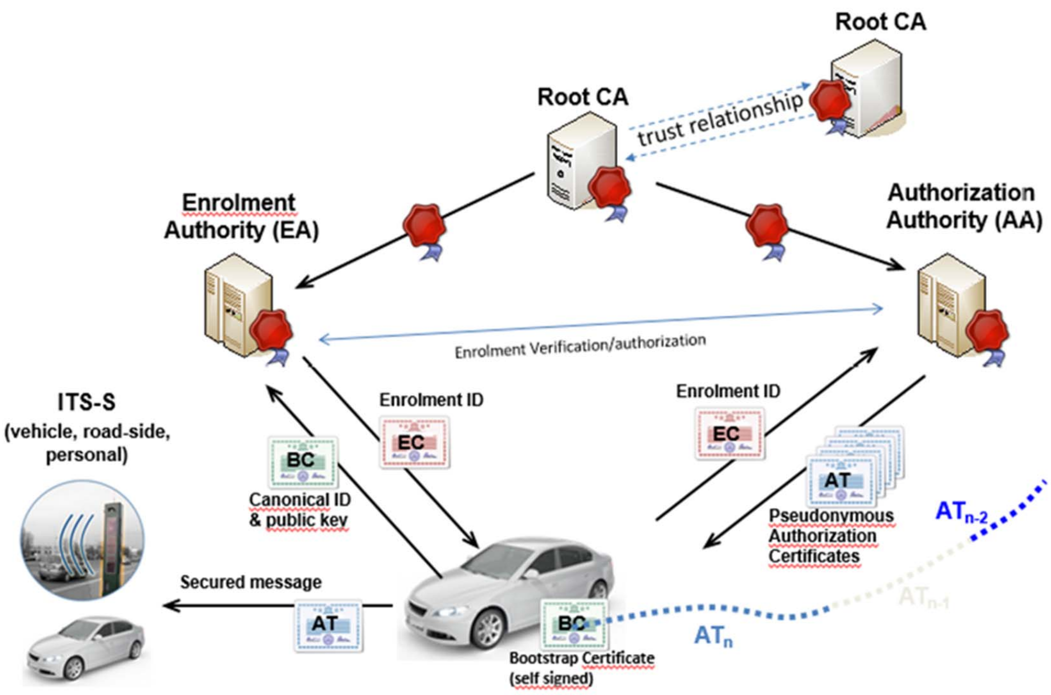
Root CA
Root CA
trust relationship
Enrolment Authority (EA)
Authorization Authority (AA)
Enrolment Verification/authorization
ITS-S
(vehicle, road-side, personal)
Enrolment ID
EC
Enrolment ID
EC
BC
Canonical ID & public key
AT
Pseudonymous Authorization Certificates
AT_{n-2}
AT_{n-1}
AT_n
Secured message
AT
BC
Bootstrap Certificate (self signed)

Figure 2: ETSI ITS trust model (PKI)

ETSI design considers a hierarchical PKI structure, with the RCA acting as the trust anchor or summit of the CAs hierarchy and controlling all subordinate certification authorities and end-entities in its hierarchy. The C-ITS PKI system may consist of a number of RCAs, which may cooperate and cross-certify each other.

For example, in Europe the C-ITS Platform has specified a C-ITS Trust model option with multiple Root CAs and a Certificate Trust List managed by the top-level, governance entities.

4.3.2.3 Security profiles for CAM and DENM

The security profiles for CAM and DENM messages are defined in ETSI TS 103 097 [i.22]. As a short summary:

- When sending CAM messages:
  - An AT will be inserted every 1s or after an AT change (in the security header)
  - A digest of this AT will be used the rest of the time (in the security header)
  - A signature, generated using the private key corresponding to the AT, will be done for each CAM message (in the security trailer)
  - The generation time will be mentioned (in the security header), for plausibility check and protect against replay attacks
  - All data are in plaintext (no encryption)
- When sending DENM messages:
  - An AT will be used for each DENM message (in the security header)
  - A signature, generated using the private key corresponding to the AT, will be done for each DENM message (in the security trailer)
  - The generation time will be mentioned (in the security header), for plausibility check and protect against replay attacks
  - The generation location will be mentioned (in the security header) for plausibility check
  - All data are in plaintext (no encryption)

- When receiving a CAM or DENM message, the signature verification applied as specified in ETSI TS 102 941 [i.26]:
    - The AT validity will be checked (to ensure the originating ITS-S is authorized):
        - E.g. certificate time/geographic validity or permission levels (AID-SSP) are checked
    - The signature will be checked (to ensure authenticity and integrity of the message)
    - The validity of the chain of certificates up to a valid root of trust (RCA certificate) will be checked
    - The validity of CA certificates in the chain will be checked using the trust list and revocation list information (CRL, CTL)

The AT will be changed regularly, to avoid tracking possibility (correlation between AT and vehicle identity) and protect privacy of vehicle occupants.

When an AT change is triggered, all other ITS-S ID (e.g. StationID in CAM/DENM, GeoNetworking source address or MAC source address) are changed at the same time.

AT change triggering conditions are not currently specified in ETSI Standards.

Moreover, the previously mentioned authorization tickets have been obtained beforehand from an AA within the security management infrastructure (PKI).

4.3.2.4 Pseudonym change locking in RHS use cases

In current ETSI road safety application standards such as RHS [i.16], a pseudonym change locking mechanism is already required for CAM and DENM messages, only in the case of safety-critical situations (corresponding to "priority levels"=0 or 1, see in RHS [i.16] and LCRW [i.30] ETSI standards).

In these situations, the originating ITS station estimates that receiving ITS-Swill either require an immediate driver's action, trigger a vehicle automation action, or prepare pre-crash operations.

NOTE: Short term certificates (pseudonyms) will not be changed when the RHS application detects a critical traffic safety situation identified through the setting-up of priority levels "0" or "1".

However, driver awareness situations (i.e. priority level=2) are not concerned by such locking in ETSI standards.

The impact of the pseudonym change strategies on receiving ITS-S applications will be illustrated in clause 4.4.2.

4.3.2.5 Road safety applications requirements w.r.t. pseudonym change

Road Safety services can be classified in the three following categories:

- **Primary or active road safety** category contributing to collision avoidance between vehicles/vulnerable and between vehicles and the road infrastructure. This is including ADAS/ driving assistance and future autonomous driving.
- **Secondary road safety** category mitigating the impact of collisions when not avoidable e.g. pre-crash/post-crash systems. This includes the seat belts and airbags.
- **Tertiary road safety** category accelerating the rescue of people, involved in accidents e.g. the e-Call.

The main target of C-ITS is to highly contribute to road safety helping to avoid accidents and, in addition, to enhance the support for secondary road safety functions (pre-crash).

In the ETSI approach, the primary road safety application classification model represented in figure 3 is applied as a reference model for standardization. This figure prefigures the expected deployment steps:

- Step 1: information and cooperative awareness
- Step 2: collision avoidance based on driving assistance
- Step 3: collision avoidance based on automatic driving

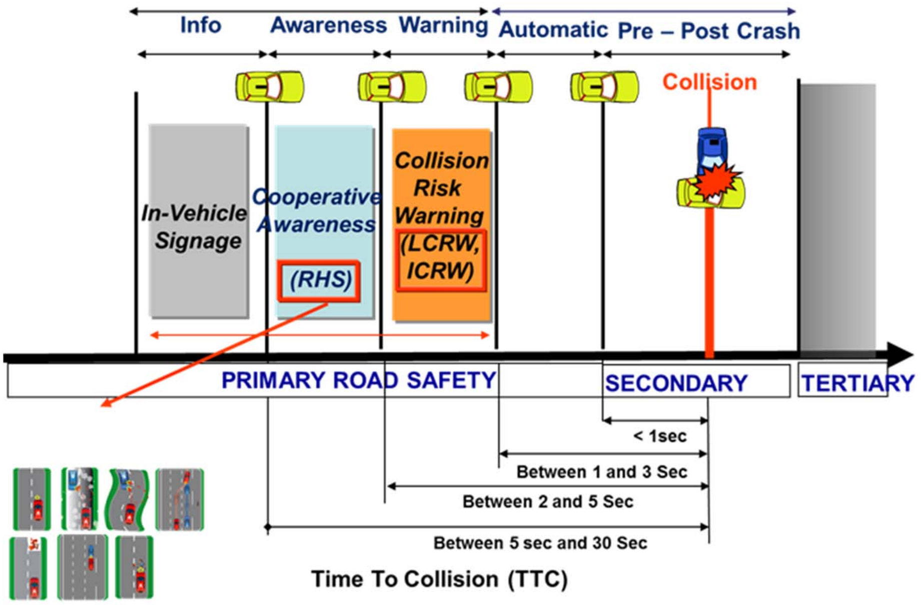

Figure 3: Road Safety Model in C-ITS

The RHS [i.16] application purpose is to create the driver awareness of a danger ahead on its vehicle trajectory. The purpose of this service is to increase the vigilance of the driver to avoid a collision, in situations, which do not require an immediate action.

The Collision Risk Warning applications (LCRW [i.30] and ICRW [i.33]) purpose is to issue warnings to the driver requiring an immediate action to avoid an accident e.g. emergency brake or stay in lane.

A direct action on the vehicle (automatically) is the ultimate goal in order to be able to reach the European Commission challenge of zero fatalities and zero serious injuries on European roads.

Collision avoidance applications are relying on the critical broadcast communications of highly dynamic information/data elements. Data elements are exchanged using standard CAM and DENM, which provide accurate and reliable vehicle velocity information including position.

Based on road safety application classification (figure 3), ETSI RHS standard specifies 3 priority levels. Table 1 provides the priority level that is being assigned according to the criticality level of the traffic safety situation, which is defined by the time to a potential collision (e.g. using calculation of Time Proximity Vector at crow flies [i.16]).

Table 1: Traffic safety situation priority level

Priority level	Critical traffic safety situation	Triggering condition	CAM interval (informative)	DENM interval
2	Driver assistance, Cooperative Awareness	10 use cases	Between 100 to 1 000 ms	Between 100 to 1 000 ms
1	Driver assistance or automatic action	Driver warning if TTC < X1 (e.g. 5 s) Direct action if TTC < X2 (e.g. 1 s)	Between 50 to 100 ms	=< 100 ms
0	Pre-crash situation		Between 50 to 100 ms	=< 100 ms

The data quality elements to be considered are:

- The accuracy of dynamic data elements and in particular the positioning of the vehicles.
- The confidence level of received data elements accuracies.
- The age of received data elements at the receiving level e.g. less than 300 ms [i.16].

The age of data is depending on the frequency of data, the packet losses and the latency time of the whole end-to-end system. ETSI TS 101 539-3 [i.30] estimates this end-to-end latency time for critical safety situations (maximum end-to-end latency time of 300 ms at a maximum CAM/DENM frequency of 10 hertz).

When the receiving vehicle detects an imminent risk of collision (priority level 0/1), a critical part in the C-ITS will be the receiving ITS-S which may have to process a high number of received messages (e.g. 1 000 per second in case of about 100 surrounding vehicles in the ad-hoc network). In such case, the processing capability of the receiving ITS-S should be sufficient and such level of performance leads to the development of specific strategies for the verification of messages: e.g. message authenticity policy applying a verify on demand in US (i.e. the application decides whether the message is important and should be verified or not) or (randomly) probabilistic verification in PRESERVE project.

ETSI standards provide pseudonymous broadcasting communications for safety messages (CAM, DENM). However, the fundamental principle of road safety applications is to track the trajectories of surrounding vehicles to assess a risk of collision and avoid it. Consequently, vehicles need to be identified by pseudonyms being changed according to some rules.

When a vehicle is in a critical safety situation (level 0/1), the pseudonyms which are used to track the vehicles will not be changed. This is critical because there is a risk of temporarily losing the tracked vehicle and not reacting properly to avoid collision.

For the same purpose, during critical safety situations, the CAM and DENM will keep the same pseudonym (stationID) because the receiving ITS-S vehicle is using simultaneously data elements which are provided by CAMs and DENMs.

The linking of the vehicle communication via its pseudonym during a short time period is also needed by traffic management applications to collect travel time information on road segments.

4.3.3 European Commission policies

The European Commission recently released two documents describing the European certificate and security policies. These documents are results from the C-ITS Platform.

Basically speaking, the Security Policy [i.36] recommends a pseudonym change strategy based on the one proposed by C2C-CC (see clause 4.2.3.2). The definition of pseudonym parameters as well as their assigned values are provided in the Certificate Policy document [i.37]. Those values can be found in table 4 of the present document.

4.4 Issues & Discussion

4.4.0 General

The pseudonym change mechanism copes well with the tracking issue but also raises non-trivial drawbacks that have to be taken into account. The following clauses describe them.

4.4.1 ID change impacting sender behaviour

Each layer of the V2X communication stack has its own identifier. Therefore even if an ITS-S changes its pseudonym, it is still possible to track it by looking at its communication IDs: the *StationID* (Facility layer), the *Geonet address* (Network & Transport layer) and the *MAC address* (Access layer).

The countermeasure of this issue is to change all IDs of the communication stack when changing pseudonym. This implies that the emission of messages is blocked during the stage of changing pseudonym and IDs. Otherwise there is a risk that two consecutive messages are sent with a part of the IDs that are identical (because not changed yet) and the other part that are different, making possible the linkability between old and new IDs.

Consequently, the process of changing pseudonym and IDs generates additional latency. However, that this latency should be largely less than 100 ms (the maximum CAM frequency) thus this process should not impact safety applications.

Also note that, as specified in clause 11 of ETSI TS 102 636-6-1 [i.28], the IPv6 address of the OBU will be changed as well as it is linked to both MAC and Geonet addresses.

4.4.2 Misleading neighbour vehicles in safety situations

In current deployment projects there are requirements to avoid change of pseudonym for a short-term period, when a car is sending DENM for alerting road hazards as it may also have potential safety consequences.

If the car finds itself in a dangerous situation (e.g. collision avoidance), it should not change the pseudonym in use for signing safety messages (CAM, DENM). A pseudonym change in a dangerous situation may provoke uncertainty for other vehicles and sending vehicle can mislead other vehicles, especially in the case where the pseudonym change strategy implies a silent period.

Figure 4 illustrates the impact of a pseudonym change followed by a silent period on the cooperative awareness of neighbouring ITS-Ss. This raises two issues:

1) **Ghost vehicles:** When an ITS-S changes pseudonym its old identity remains for a certain amount of time in the LDM of its neighbouring ITS-Ss. For instance, in the left part of figure 4 the Ego vehicle has three entries for vehicle A and two entries for vehicle B in its LDM. It may interpret that it has six neighbours, whereas in reality only two vehicles are present (black A and B). The four red A and B vehicles are ghost vehicles generated by the change of pseudonym by both vehicles A and B.

2) **Missing vehicles:** When an ITS-S observes a silent period after a pseudonym change, it does not send any V2X message. As a consequence, it is not present in the LDM of neighbouring ITS-Ss. When the silent period expires it sends back V2X messages and thus suddenly appears in the LDM of neighbouring ITS-Ss. This may generate sudden and inappropriate reactions from neighbouring ITS-Ss, leading to dangerous situations. Moreover, this may also be interpreted by neighbouring ITS-Ss as a cyber-attack. The sudden appearance of an ITS-S that was previously non-existent is indeed a non-coherent behaviour. For instance, the right part of figure 4 illustrates a missing vehicle situation. The white vehicle on the left is out of radio range of the Ego vehicle and changes its pseudonym. It then enters a silent period during which it overtakes the yellow van. When the silent period expires, it starts sending V2X messages again but it is already in the very close neighbourhood of the Ego vehicle that just initiated a lane change manoeuvre.

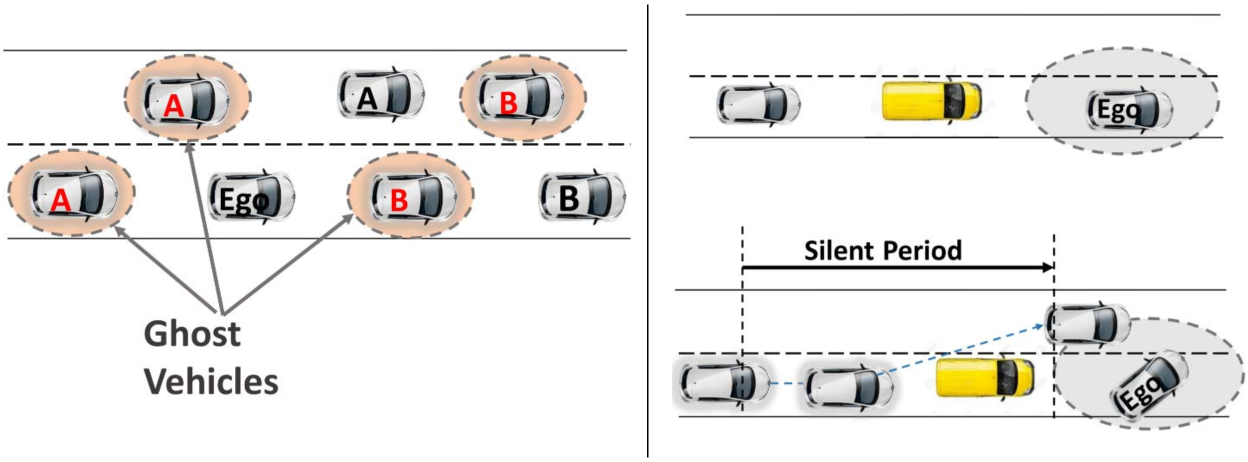

Figure 4: Pseudonym change impact on neighbourhood: ghost (left) and missing (right) vehicles

4.4.3 Trade-off between safety and privacy

The pseudonym change mechanism improves privacy by making tracking more difficult. It relies on the fact that linking two different digital identities to a same physical moving ITS-S is not an easy task. Therefore, *the more often an ITS-S changes its pseudonym, the higher its privacy*. Changing of pseudonym at each message sent seems to be the solution to reach the higher level of privacy. However, such frequent changes cause a major problem from a safety point of view.

The "neighbourhood awareness" of ITS-Ss is based on their received V2X messages. That is, an ITS-S that receives V2X messages with different identities will consider them as coming from distinct ITS-Ss and will update its cache accordingly. Therefore, if an ITS-S changes its pseudonym too frequently (e.g. at each message), a receiving ITS-S will consider that there are many different ITS-Ss in its neighbourhood whereas there is only one present physically. As safety applications rely on that "neighbourhood awareness" to take decisions, they may react to non-existent situations that may have disastrous consequences. Thus, *the less often ITS-Ss change their pseudonym, the better the accuracy of safety applications*.

Consequently, there is a need to find the best trade-off between safety and privacy when designing a pseudonym change strategy.

4.4.4 The Sybil attack

ITS-S should be able to change their current pseudonym frequently to avoid tracking. That means that ITS-S should always have access to new valid pseudonyms. This can be achieved by two ways:

1) ITS-S are able to request new pseudonyms to the PKI at any time (i.e. ITS-S are constantly connected to the Internet).

2) ITS-S have a pool of pre-requested pseudonyms that are available for use.

As the first solution is most probably not feasible, the second one is considered: when ITS-S are connected to the PKI they request several pseudonyms (pseudonym pool) for later use. The number of pseudonyms requested is configurable and will probably depend on the pseudonym change strategy that is in use: if the strategy requires very frequent pseudonym changes, the pseudonym pool size should be large whereas on the other hand, if pseudonyms are changed less frequently the pool size may be smaller.

Basically speaking the Sybil attack consists of the simultaneous use of multiple pseudonym identities by a unique entity (the attacker). Brought back to the C-ITS context, the attack consists of a malicious ITS-S using several of its pseudonyms at the same time to simulate multiple (fake) ITS-S. For instance, this attack can be used by a vehicle to make receiving vehicles and infrastructure believe that a traffic jam is occurring. As a result, neighbouring ITS-S will get a warning to slow down or they may be redirected by the traffic management entity.

The strength of a Sybil attack is related to the number of valid pseudonyms available: the more available pseudonyms an ITS-S has and are valid at a certain time, the stronger the Sybil attack it may generate. One simple countermeasure to this attack would be to limit the number of concurrently available pseudonyms. For instance in IFAL (see clause 4.2.4) the number of concurrently valid pseudonym can be limited to one. In reality the number should be two to allow for a dynamically timed pseudonym change for reasons of road safety.

The main risk of multiple concurrently available pseudonyms is that an attacker could switch between the different pseudonyms fast enough to generate plausible movement patterns for all (fake) vehicles at the same time. Therefore, an attacker needs to be able to change to a different certificate and return to the previous one in time to keep up/continue with the movement pattern.

Assuming that it is easier for an attacker to manipulate applications on the application layer than to manipulate the pseudonym certificate providing and message signing subsystem, there are possibilities to counter Sybil attacks: on the one hand, you can add a parameter that enforces a minimum duration a pseudonym certificate needs to be in use before the next pseudonym certificate can be requested. If the minimum usage duration is long enough (a few seconds should be sufficient), the attacker cannot simulate plausible movement patterns of multiple vehicles at once. Also, a minimum usage duration makes it easier for a receiver to detect manipulated vehicles (that ignore this duration). On the other hand, selective switching between the different pseudonyms can be restricted. If the pseudonym providing subsystem forbids the selection of the next pseudonym and enforces a random pseudonym, an attacker would need to cycle through all pseudonyms in order to get back to the one he needs.

4.4.5 Pseudonym lock

4.4.5.1 Current status

As presented in clause 4.3.4.2 the current security related ETSI standards require that the pseudonym change service can be locked on demand (e.g. upon request from a safety application). The related deliverables are:

- ETSI TS 101 539-1 (RHS application) [i.16]:
  - Clause 7.2.1 specifies that when a RHS application detects a critical safety situation of priority levels "0" or "1", the pseudonym change service will be locked. No information about the lock duration are provided in this document.

- ETSI TS 102 723-8 (SN-SAP specification) [i.27]:
    - The deliverable specifies the SAP between the Security layer and the Networking and Transport layer. More precisely, SN-SAP defines the *SN-ID-LOCK* service (clause 5.2.9) that enables to ask the Security layer to lock the pseudonym change process for a specific period of time. The pseudonym change process is then automatically unlocked when the period of time elapsed. It can also be manually unlocked by using the *SN-ID-UNLOCK* service (clause 5.2.10).
    - According to clause 5.2.9.2, the period of time for pseudonym lock is provided in seconds and encoded on one byte. That is, the maximum amount of time that can be requested is 255 s.
    - The Security layer acknowledges the reception of a *SN-ID-LOCK* request by giving back the corresponding *lock_handle*. This parameter is required for manual unlock via the *SN-ID-UNLOCK* service.

In the US, the SAE J2945/1 [i.31] standard also defines the possibility to lock pseudonym change when a safety application detects a dangerous situation ("alert" mode). However, the triggering conditions to enter in the "alert" mode are not defined yet.

The C2C-CC also considers pseudonym lock and proposes in their BSP document a maximum lock time of fifteen minutes. However discussions are on-going to revise this value to a maximum lock time of five minutes.

4.4.5.2 Issue

The pseudonym change lock functionality, as described in the current version of the security related ETSI specifications above mentioned, raises a privacy issue. It is indeed possible for an application to lock the pseudonym change for an infinite amount of time: whenever the lock timer is ready to expire, the application reset the timer by requesting again a lock. The ITS-S is thus prevented to change its current pseudonym, making it easily trackable.

One possible solution to this issue could be to allow the Security layer to refuse an incoming SN-ID-LOCK request. For instance, an application that already requested a SN-ID-LOCK and requests again another one before the first one expired may be refused. However, as the maximum authorized lock time is 255 s [i.27], the Security layer should not prevent safety applications to continuously lock pseudonym change until the situation becomes safer. To this end, an authentication mechanism could be put in place at the Security layer level to differentiate legitimate applications (e.g. RHS) from other applications (e.g. third-party). The former should be authorized to lock the pseudonym change as long as necessary whereas the latter should not (indeed third-party applications should not be trusted and thus considered as potentially malicious applications).

In addition, before authorizing a pseudonym lock the Security layer should ensure that the pseudonym remains valid for the period of lock time requested. This is needed in order to avoid the situation where the current pseudonym expires (end of validity period) and has to be changed while it is locked.

4.4.6 Pseudonym reuse

Pseudonym reuse consists of authorizing ITS-Ss to use a pseudonym that they already used previously, as long as its validity period has not expired. For instance, an ITS-S may use pseudonym A for a time, then change to pseudonym B, and then change back to pseudonym A. This adds flexibility to pseudonym changes by reducing the required pseudonym pool, thus reducing pseudonyms requests to the PKI and the embedded memory storage. However the drawback is that it has a bad impact on privacy as it becomes easier to track a vehicle by linking space and time data tuples when the vehicle used the same pseudonym.

Not authorizing pseudonym reuse is obviously the best practice to preserve privacy. However, this also implies that ITS-Ss request new pseudonyms to the PKI more often and embed more memory to store bigger pseudonym pools. The financial cost of downloading new pseudonyms may also be a non-negligible factor since non-reuse strategies will consume more pseudonyms.

Whether pseudonyms should be reused or not is still an open question. Reuse provides more flexibility but makes the design of pseudonym change strategies more complex (as it has to cope with the privacy issue) whereas non-reuse provides better privacy but at the cost of higher pseudonym consumption.

The C2C-CC considers the reuse of pseudonyms in the pseudonym change strategy they propose (see clause 4.2.3.2). They propose several solutions to manage the pseudonym pool to ensure that pseudonym reuse has the least possible impact on privacy. In order to evaluate the privacy efficiency of those solutions they provide four specific KPIs. The details of these KPIs are in clause 5.1.4.

5 Metrics for performances evaluation & comparison

5.1 Metrics for privacy assessment

5.1.1 General

In the present document only privacy related to pseudonym management is being considered. This means that the efficiency of a pseudonym change strategy in terms of linkability is evaluated. (i.e. is it easy for an eavesdropper to link pseudonyms of an ITS-S that just changed?). Privacy related to the messages themselves and their content are not considered.

5.1.2 Anonymity-based metrics

5.1.2.1 Definition of anonymity

The notion of *anonymity* has been defined in [i.6] as "*the state of being not identifiable within a set of subjects, the anonymity set* where *anonymity set*" represents a set of subjects that may be related to an anonymous transaction.

5.1.2.2 Definition of entropy

The *entropy* is a measure of the uncertainty of a random variable. For example, let us define *X* as a random discrete variable and p_i represents the probability that *X* takes the value of *i*, where *i* represents all the possible values that *X* can take with $p_i > 0$. *H(X)* represents the entropy of *X* and is computed using the following formula:

$$H(X) = -\sum_{i=1}^{N} p_i \log_2(p_i)$$

with *N* representing the number of subjects in the anonymity set.

Based on the entropy, authors of [i.7] and authors of [i.8] propose each a metric to measure the anonymity of a system: the *effective anonymity set size* and the *degree of anonymity* respectively. In reality the latter is a normalized version of former. According to [i.8], the definition of both metrics is detailed below.

5.1.2.3 Metric 1: Effective anonymity set size

Consider an anonymity system composed of *Ψ* users. One of those users sends a message *M* and an attacker wants to know which user it is. After deploying its attack on the system the attacker gets a probability distribution that links each user *u* to the role of being the sender of *M*. In other words, depending on the information gathered with the attack, the attacker assigns to each user *u* a probability p_u that reflects its view of *u* being the sender.

In order to evaluate the anonymity of the system (i.e. the difficulty for the attacker to determine which user *u* sent *M*), authors of [i.7] defined the *effective anonymity set size S* as a metric. *S* is equal to the entropy of the anonymity set and is computed as follows:

$$S = -\sum_{u \in \Psi} p_u \log_2(p_u)$$

That is, $0 \leq S \leq \log_2|\Psi|$ where:

- $S = 0$ means the system provides no anonymity
- $S = \log_2|\Psi|$ means the system provides maximum anonymity

5.1.2.4 Metric 2: Degree of anonymity

Authors of [i.8] go a step further and propose the *degree of anonymity* as a metric. They define the degree of anonymity as a normalized version of the effective anonymity set size, thus bounding its value between 0 and 1. The degree of anonymity d is computed as follows:

$$d = 1 - \frac{S_M - S}{S_M} = \frac{S}{S_M}$$

where S_M is the maximum effective anonymity set size.

S_M is reached when the system provides maximum anonymity, i.e. when the probability distribution is uniform ($p_u = 1/\Psi$). As mentioned previously, S_M is computed as follows:

$$S_M = \log_2 |\Psi|$$

5.1.2.5 Example of application on pseudonym change strategies

The degree of anonymity can be used to evaluate the level of privacy provided by the different pseudonym change strategies. To this end, the following scenario can be considered.

An attacker is tracking a vehicle *v* by eavesdropping the traffic in the C-ITS network. At some point, *v* changes its pseudonym according to the pseudonym change strategy under test. After that, is the attacker able to link *v* with its new pseudonym?

The computation of the degree of anonymity *d* will answer this question. To this end, the parameters summarized in table 2 will be used.

Table 2: Parameters settings to compute *d*

Attacker objective	Tracking of vehicle *v*
Attack type	Eavesdropping
Anonymity set size (Ψ)	*v* + all nearby vehicles
Event triggered	*v* changes its pseudonym
Probability distribution (p_u)	After the event is triggered, the attacker assigns a probability p_u to each vehicle in Ψ that represents his view of the vehicle being the one he is tracking
Level of privacy reached	Computation of *d*

5.1.3 User-centric metrics

5.1.3.1 Metric 1: Location privacy model

Consider a mobile network of *n* nodes. The location privacy represents the level of privacy that a node n_i currently has. The location privacy increases linearly over time: when n_i just changed pseudonym, its location privacy is strong because an attacker cannot track it (considering that the attacker cannot link the previously used pseudonym with the new one). The more elapsed time since n_i changed its pseudonym, the weaker its location privacy becomes. That is, by evaluating the distance over which it is trackable, n_i can compute its current location privacy.

User-centric location privacy is a distributed approach where nodes of the mobile network trigger a pseudonym change based on their computed location privacy.

Authors of [i.13] propose to model the evolution of the user-centric location privacy level over time. To this end, they introduce first the *location privacy loss function* $\beta_i(t, T_i^l)$ that models the location privacy level of a node *i* as follows:

$$\beta_i(t, T_i^l) = \begin{cases} \lambda_i . (t - T_i^l)\, for\; T_i^l \leq t < T_i^f \\ A_i(T_i^l)\, for\; T_i^f \leq t \end{cases}$$

where:

- t is the current time
- T_i^l is the time of the last successful pseudonym change of node *i* ($T_i^l \leq t$)
- T_i^f is the time when the location privacy loss function is maximal ($T_i^f = \frac{A_i(T_i^l)}{\lambda} + T_i^l$)
- λ_i is a sensitivity parameter that models the tracking power of the attacker as believed by node *i* (the higher the value of λ_i, the faster the rate of privacy loss increases)

They then compute the *user-centric location privacy* $A_i(t)$ of a node *i* at time *t* as follows:

$$A_i(t) = A_i(T_i^l) - \beta_i(t, T_i^l), t \geq T_i^l$$

5.1.4 Pseudonym reuse KPIs

The C2C-CC proposed a pseudonym change strategy that authorizes pseudonym reuse. They defined the following KPIs to limit the impact on privacy.

- **KPI 1:** The probability that the pseudonym that has been used for the first segment of a selected trip is re-used for the last segment of the same trip should be lower than 2 %.
- **KPI 2:** The probability that the pseudonym that has been used for the first segment of a selected trip is used for the mid segment of the same trip (and not for the last segment) and the probability that the pseudonym that has been used for a mid-segment of a selected trip, is (later on) used for the last segment of the same trip, should be lower than 20 %.
- **KPI 3:** The probability that a pseudonym, that has been used either for the first or for the last segment of a selected trip, has been used before or is re-used later for at least one first or one last segment of another trip should be lower than 40 %.
- **KPI 4:** The probability that a pseudonym, that has been used either for the first or for the last segment of a selected trip, has been used before or is re-used later at least once for any mid segment of another trip (and NOT for the first or last segment of another trip) should be lower than 40 %.

These KPIs have been defined specifically for the C2C-CC pseudonym change strategy and thus may be modified/adapted to fit other strategies.

5.2 Metrics for safety assessment

5.2.1 General

There are several works in the literature that focus on the performances evaluation of safety applications in VANETs (Vehicular Adhoc NETworks) environments [i.9], [i.10], [i.11] and [i.12]. They consider that safety applications rely either on the periodic broadcast of one-hop messages or on the emission of multi-hops alert messages when a dangerous situation occurs (typically these two safety messages correspond to CAM and DENM respectively). Therefore, the recurring metrics considered to evaluate the performances of such safety applications are the *reception (or delivery) rate* and the *latency*.

The following clauses provide a description of relevant safety metrics. Metrics are classified in two categories: network-level and application-level.

5.2.2 Network-level metrics

5.2.2.1 Metric 1: Reception rate/packet losses

The reception rate or packet loss is computed as the ratio of the amount of messages received by an ITS-S to the total amount of messages that it should have received. This metric has an impact on safety as the more messages an ITS-S receives, the more up-to-date information it gets, thus leading to safer driving.

Pseudonym change may increase packet losses because of the communication stack flushing operation: when a pseudonym change occurs, the communication stack will change all of its IDs. But before changing them, the stack will need to be flushed. That is, all messages that are on the way to be sent are dropped instead.

5.2.2.2 Metric 2: Delay/latency

Delay is a well-known metric that consists of measuring the amount of time elapsed between the sending of a message by an ITS-S and its reception by another one. In real-time applications (such as safety applications) minimizing the delay is of paramount importance. The earlier an ITS-S receives an information, the more time it has for reacting accordingly.

The pseudonym change mechanism includes the prevention of sending of new V2X messages before all IDs of the communication stack are changed, thus introducing delays. Therefore, it has to be ensured that the mechanism of changing pseudonym still satisfies the safety applications requirements in terms of delay.

5.2.2.3 Metric 3: Wireless channel overhead

Vehicles send frequently their certificates when sending CAM messages. When a vehicle changes its pseudonym, it has to send its full certificate. Frequent pseudonym change may create overhead on the wireless channel and may degrade the performance of the safety application. Overhead due to pseudonym change can be calculated as the ratio between the data sent when there is no applied pseudonym change and the data sent when pseudonym change is performed.

5.2.3 Application-level metrics

5.2.3.1 Metric 1: Message inter-arrival duration

At a receiving ITS-S, the message inter-arrival duration is the amount of time elapsed between the receptions of two consecutives messages coming from a same ITS-S source. This metric gives an indication about the "freshness" of the information received by the ITS-S.

Pseudonym change has a direct impact on message inter-arrival duration since when an ITS-S changes its current pseudonym, it also has to change all of its identifiers before being able to send a new message. Therefore, the time elapsed between the sending of two consecutive CAM increases when a pseudonym change takes place. This time increases even more if the pseudonym change strategy implements a silent period.

5.2.3.2 Metric 2: Cooperative awareness quality

Cooperative awareness quality is the ability of each vehicle to have a near-to-reality image of its dynamic environment based on information received from other vehicles. Dynamic elements of the environment are for instance moving vehicles, pedestrians, cyclists, etc. Information is transmitted in the CAM messages and is stored in a specific database such as the LDM (Local Dynamic Map). ITS Applications use this database to perform internal calculation of road potential risks.

When a vehicle changes its pseudonym, it sends a CAM message with the new identity. For receiving vehicles, the new identity in the message means that there is a new neighbour in their vicinity. Pseudonym change may affect the cooperative awareness by leading vehicles to an irrelevant dynamic environment awareness.

The cooperative awareness quality can be measured as the deviation of the vehicle's dynamic environment awareness from the real dynamic environment situation. The bigger the deviation is the worse the cooperative awareness is.

Authors of [i.17] introduced the quality of cooperative awareness. Basically speaking, the awareness of vehicle *i* at time *t* and within distance *d* is computed as follows:

$$Awareness_{d,t}(i) = \frac{\left|N_i^d(t)\right|}{\left|V_i^d(t)\right|}$$

where N_i^d is the set of all discovered neighbors by vehicle *i* within distance *d* and V_i^d is the set of all vehicles physically present within distance *d*.

It is also possible to calculate the average deviation ratio of the cooperative awareness with respect to a communication range R of all existing vehicles in the network C (i.e. $d = R$) as the average value of all calculated deviation ratio of each vehicle in a given period T.

$$Average\ Awareness\ Deviation\ ratio = \frac{\sum_{t=1}^{T} \frac{\sum_{i=1}^{C} \left|1 - Awareness_{R,t}(i)\right|}{C}}{T}$$

5.2.3.3 Metric 3: Application Reliability

As introduced by paper [i.21], the *T-window* reliability is defined as the successful reception of at least one single packet from neighbour vehicles during the tolerance time window T. The application is claimed to be reliable if at least one packet is received during the tolerance window. Different applications have different tolerance windows and the shorter the tolerance window is, the harder the delay requirements are. The *T-Window* reliability is calculated as the ratio of the number of reliable time instances to the number of all-time instances.

5.3 Metrics for cost assessment

The cost of a pseudonym change strategy is also a metric that should be considered in the evaluation process. Strategies that do not allow pseudonym re-use or that change pseudonym very frequently would indeed have an impact on the TCO.

Currently the only studies that are available on this topic come from NHTSA [i.34] and C-ITS Platform [i.35]. Both use the OPEX and CAPEX KPIs for cost evaluation. There are also on-going studies in France, especially in the framework of SCOOP@F project.

6 Evaluation

6.1 General

Clause 6.2 presents the evaluation of pseudonym change strategies that have been identified in the present document. In the present document this evaluation is not available. It is part of the second step of the present document and thus will be provided in a future release.

6.2 Void

This clause is reserved for the evaluation.

7 Pseudonym lifecycle

7.1 General

Clauses 7.2 describes the parameters for the control of the full pseudonym lifecycle. The objective is to find a compromise on the boundaries for pseudonym parameters in order to meet security and privacy protection targets. At the same time there may be some room for difference in pseudonym parameters - within these boundaries - in order to enable C-ITS stakeholders to make trade off decisions between risks and costs.

The structure is that first all parameters that control the pseudonym lifecycle will be listed and defined. Then in a future step when the evaluation will be done, the ranges of allowed values of these parameters will be specified. Clause 7.3 provides pseudonym parameters values of some C-ITS early implementations. Note that these values (also provided in Annex A) are for reference purposes only.

7.2 Parameters definitions

Table 3 gives an overview of pseudonym lifecycle management parameter definitions.

Table 3: Overview of pseudonym lifecycle management parameter definitions

Parameter		Definition
(EC Lifetime Period)		The duration between the starting date and the expiration date of the EC.
Validity period (or pseudonym lifetime)		The validity period of a pseudonym is the duration between its starting date and its expiration date. The validity period should not exceed the EC lifetime.
Minimum pseudonym lifetime overlap		The minimum overlapping period between succeeding pseudonyms in order to allow pseudonym change while vehicle is driving/ ignited; this time will be added to pseudonym end-date-time. Pseudonym overlap should not exceed the maximum parallel number of pseudonyms.
Maximum number of parallel pseudonym		The number of pseudonyms within one ITS-S that are valid at the same time. This value includes the overlap time.
Maximum number of parallel pseudonym with the same validity period		The number of pseudonym's that expire at the same timestamp. Ideally this number should be one in order to prevent linking of pseudonyms to one individual vehicle.
Usage	Pseudonym Min use time before pseudonym change	The minimum duration that the pseudonym is used for signatures until allowing another pseudonym change (see clause 4.4.4).
	Pseudonym Max use time before pseudonym change	The maximum duration that the pseudonym is used for signatures until next change (whatever comes first between time or distance).
	Pseudonym Max use distance before pseudonym change	The maximum distance that the pseudonym is used for signatures until next change (whatever comes first between time or distance).
	Any other parameter for pseudonym change	Any other parameter can be used (e.g. number of signatures) to change the pseudonym earlier than time or distance.
Pseudonym Max reuse number		The maximum number of reuses of the pseudonym (if specified).
Pseudonym Preloading Period		The maximum duration during which an ITS-S can request pseudonyms with a validity period that has not started yet.
Pseudonym refilling scheme communication profile (ETSI TS 102 941 [i.26])		The communication network (Wi-Fi, ITS-G5, cellular, etc.) that accesses the ITS station to load additional pseudonym's.
Pseudonym batch size		The number of pseudonym that are provided upon a single pseudonym request from the ITS station.
Any other rule for pseudonym certificate change (criteria, boundary)		The rules for pseudonym change that are not related to time and distance (e.g. change at ignition).
Selection of next pseudonym when a change applies		How the ITS-S selects its next pseudonym (e.g. random, round-robin, etc.).
Pseudonym minimum time window before its next use		The minimum amount of time an already used pseudonym cannot be used again.
Maximum pseudonym change lock duration		ITS-S suspends pseudonym change during the lock time du to application conditions.

7.3 Examples of parameters values

Table 4 shows the parameter values that are defined by current C-ITS projects and SDOs.

Table 4: Examples of pseudonym parameters values from C-ITS projects and normative organizations

Parameter	SCOOP@F	C2C-CC	SAE	ETSI	IFAL	CAMP	EC CP/SP
Validity period	1 week	1 week		Not defined	12 minutes	1 week	1 week
Max number of parallel pseudonyms	10	60		Not defined	2	20	- vehicle ITS-S: 100 - roadside ITS-S: 2 per ITS-AID
Pseudonym Lifetime overlap	Yes	Yes		Not defined	Yes		
Usage	After 40 000 signatures			Not defined	12 minutes		
Pseudonym Max reuse number	Round-robin method			Not defined	0	Random	
Pseudonym pool size	260	60		Not defined	2		
Pseudonym Preloading Period	6 months	36 months		Not defined	10 years	1 year	3 months
Rule for pseudonym certificate change (criteria, boundary)	- Ignition - After 40 000 signatures	- Ignition (if engine deactivated for at least 10 minutes AND movement detection) - First change after 800 to 1 500 m - Next changes after at least 800 m and an additional interval of 2 to 6 mins	- Ignition - Every 5 minutes	Not defined	- Rotation every 10 minutes in order of their validity time window	- Rotation every 5 minutes based on a dynamic choice - Mix-Zone approach (study ongoing)	- Ignition (if engine deactivated for at least 10 minutes AND movement detection) - First change after 800 to 1 500 m - Next change after at least 800 m and an additional interval of 2 to 6 mins - Next change after 15 km ± 5 km (randomly) - Further changes after 30 km ± 5 km (randomly)
IDs changed upon pseudonym change (see note below the table)	- StationID - @IPv6 - @GN - @MAC - Path history reset	- StationID - @GN - @MAC - Path history reset	- DE_Msg Count - DE_Temporary_ID - @MAC	- StationID - @IPv6 - @GN - @MAC			
Lock of pseudonym change	When sending DENM message	15 minutes on request of safety applications (unlimited in stationary vehicle)	See clause A.3	Lock ID Change with max duration of 255 s at SN-SAP [i.27]			

NOTE: ETSI TS 102 723-8 [i.27] specifies the SN-IDCHANGE-TRIGGER service but it is currently not used.

8 Conclusions and Recommendations

The present document has described the current advances on pseudonym change management and the different strategies have been evaluated. Table 5 and table 6 present the pseudonym parameters evaluation framework as well as the recommendations for coping with the identified issues which will need to be considered in ETSI ITS standardization work.

Table 5: Pseudonym parameters evaluation framework

Objective	Explanation	Parameters	KPI
Safety Operational performances	The use of pseudonym for safety messages communication on ITS-G5 needs to meet the requirements of road safety & traffic management applications and fulfil the level of quality of ITS information transmitted by ITS stations (delay, trust, awareness aspects) while preserving the privacy of vehicles/users and will have impacts on the societal benefits for Road-Safety [i.35].	All	Decrease of the expected accident reduction rate (due to the changing of pseudonyms in the safety messages communication). Decrease of the gains in Euros (savings in terms of reducing fatalities, serious/minor injuries and material damages).
Privacy protection	The purpose of pseudonyms is to not reveal identities nor individual trip histories and is the more effective the shorter the use of an individual pseudonym is.	The pseudonym Max use time before pseudonym change, The pseudonym Max use distance before pseudonym change, Any other parameter for pseudonym change, pseudonym Max reuse number, Maximum pseudonym change lock duration, pseudonym minimum time window before next use, pseudonym batch size.	Max. exposure of a single pseudonym to C-ITS receivers.
Revocation	Trust is dependent of how quickly malfunctioning ITS stations can be stopped; Besides physical intervention of the station itself the revocation can be done remotely by impacting the pseudonym's.	Pseudonym Lifetime, pseudonym Preloading Period (pseudonym certificates tank).	Max throughput time that an ITS station can be prevented to use valid pseudonyms.
Mitigate identity attacks	When ITS stations have more valid pseudonym's at the same time they may use them all at once and pretend to be multiple ITS stations (Sybil attack risk).	Maximum number of parallel pseudonym's, The pseudonym Min use time before pseudonym change.	Max. number of concurrently valid pseudonyms of a single ITS station.
Operational pseudonym costs	The TCO of vehicular ITS-S or roadside ITS-S. Note that the roadside ITS-S may have a secondary function i.e. the distribution of pseudonyms.	Pseudonym Lifetime, Maximum number of Parallel pseudonym, The pseudonym Max use time before, The pseudonym Max use distance before pseudonym change, Any other parameter for pseudonym change, pseudonym refilling scheme distribution channel, pseudonym Preloading Period (pseudonym certificates tank), pseudonym batch size.	CAPEX and OPEX costs in Euros for one year of pseudonyms.
Reliability of pseudonym security implementation		Pseudonym refilling scheme communication profile (ETSI TS 102 941 [i.26]).	Likelihood of a weak security implementation.

Table 6: Recommendations

Recommendation	Explanation
Information included in a pseudonym	ITS-S provide their full pseudonym certificate in V2X messages (always in DENM, and one out of 10 CAM). The information included in the messages should not enable the linkage between different pseudonyms coming from a same ITS-S. However, a pseudonym certificate includes the HasedID8 of the AA that provided the certificate. This information may be used to link pseudonym coming from a same AA. This AA information is important for security as this AA information should be compared to the CRL (it is one of the steps in the validation of the certificate chain ETSI TS 102 941 [i.26]).
Pseudonym lock duration	The pseudonym lock functionality is a necessity as changing pseudonym in a critical situation may be dangerous. The related ETSI standard needs to specify in due course a maximum SN-ID-LOCK time in order to prevent infinite pseudonym change locks. The current recommendation would be 15 minutes in order to comply with current best practices.
Sybil attacks	In order to prevent Sybil attacks and their potential traffic impact and attacker motivation a variety of counter measures is recommended. The present document shows that several counter-measures exist to mitigate the risk. Thus risk evaluation should take them into consideration. For instance, the number of concurrently valid pseudonym certificates for each individual ITS-S would be very low [i.29]. Ideally the minimum value for this parameter would be 2 in order to allow dynamic timing for pseudonym change. Other measures would be application validation of used pseudonym identities and misbehaviour detection and enforcement.

Annex A:
Parameters of C-ITS early implementations

A.1 SCOOP@F project

Table A.1 presents the parameters for the pseudonym change strategy considered in SCOOP@F project.

Table A.1: SCOOP@F pseudonym change strategy parameters

Change of addresses/identifiers	Station ID, MAC address, GN address, IPv6 address
Lifetime of pseudonym (time slot)	1 week for vehicles
Number of parallel pseudonym (issued to be valid in the same time interval)	10
Pseudonym preloading interval	6 months
Pseudonym change method	Round-Robin
Pseudonym change criteria	After 40 000 signatures or 1 hour whichever is reached first and at each startup for vehicles

A.2 Car-2-Car Communication Consortium

Table A.2 presents the parameters for the pseudonym change strategy considered by the C2C-CC as specified in [i.18] and [i.19].

Table A.2: C2C-CC recommendations for pseudonym lifecycle management

Canonical ID/Key	C2C-CC PKI Pilot specifications: Canonical ID (8 Bytes OEM, 8 Bytes serial number), Canonical key NIST P-256.
Canonical ID/Key Lifetime period	OBU lifetime (10/15 years).
Pseudonym lifetime period	Defined in Certificate Policy. Maximum 1 week + overlap period.
Pseudonym lifetime overlap	Overlapping period.
Pseudonym certificate pool size	For each year about 1 040 pseudonym.
Number of pseudonym pools	1
Pseudonym Certificates tank (pseudonym preloading period)	3 years
Pseudonym refilling scheme via communication media	Many connectivity options including both on-line and off-line ([i.18]): • Wireless ITSG5/802.11p via a RSU • WLAN via a RSU, Hotspot, Home network • Cellular network • Cellular network • OBD/ diagnostic system at garage or inspection • Removable media (e.g. SD card, USB stick, smart-card) • short-range wireless link (BT, IR .) using a smart-phone • Wired or wireless connection to the electric charging station
Parallel pseudonym number	20
Rule for pseudonym certificate change	When ignition is switched on, within a max. period of 1 minute (except if it has been restarted within the last 10 minutes). Then change after a random time period between 10 to 30 minutes.
Change of addresses/identifiers	Simultaneous change of all addresses and identifiers in communication stack (StationID, GN Address, MAC Address).
Selection of next pseudonym when a change applies	Not defined.
Pseudonym certificate use limit	Same pseudonym used many times (unlimited number of uses), until end of validity.
Lock of pseudonym change	Lock on request from critical safety applications. Max 15 minutes, unlimited in the case of a stationary vehicle.

A.3 SAE

Table A.3 presents the parameters for the pseudonym change strategy recommended by the SAE.

Table A.3: SAE recommendations for pseudonym change strategies

Rule for pseudonym certificate change	At startup then every 5 minutes.
Change of addresses/identifiers	Change the following identifiers : DE_MsgCount, DE_Temporary ID and the DSRC Radio Subsystem MAC address.
Lock of pseudonym change	1) The System should not change its certificate as long as one or more Critical Event Flags are set, unless the certificate expires. 2) The System should not change its certificate if it is separated by less than *vCertChangeDistance* in absolute distance from the location at which the last certificate change occurred, unless the certificate expires, or unless shutdown and startup have occurred since the last certificate change.

History

Document history		
V1.1.1	April 2018	Publication