# Position Paper regarding personal data protection aspects in C-ITS

## CAR 2 CAR Communication Consortium

## Partners of the C2C-CC

## Document information

| | | | | | |
|---|---|---|---|---|---|
| **Number:** | TR_2045 | **Version:** | 101 | **Date:** | 2017 – 04 – 24 |
| **Title:** | Position Paper regarding personal data protection aspects in C-ITS | | | **Document Type:** | Technical Report |
| **Release:** | | | | | |
| **Release Status:** | Public sharing | | | | |
| **Status:** | Completed | | | | |

**Author:**

| Company /Institute | Author | Chapter |
|---|---|---|
| Kapsch TrafficCom | Jasja Tijink | All |
| Opel | Carsten Büttner / Peter Andres | 2.4 |
| | | |
| | | |
| | | |

**Approval:**

| Function | Name, Company | Date | Signature |
|---|---|---|---|
| General Manager | Niels Peter Skov Andersen | 24 April 17 | |
| | Technical Committee | 27 April 17 | |
| | Steering Committee | 03 May 17 | |
| | | | |
| | | | |

**Outstanding Issues**

| Issue | Author | Chapter |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |

## Changes since last version

| | |
|---|---|
| **Title:** | |
| **Explanatory notes:** | |

| Issue | Rev. | Date | Changes | Edited by | Approved |
|---|---|---|---|---|---|

# Content



# List of figures



# List of tables

# 1 Executive Summary

The C2C-CC consortium is convinced to have found a solution for user data protection in CAM and DENM transmission, considering technical and economic viability. The proposed architecture has already been incorporated in the European Certificate Policy for C-ITS. The C2C-CC Consortium recommends that the proposed practical solution is used a basis to define boundary conditions for Authorization Ticket (AT, aka pseudonym certificate) usage in the Certificate Policy. Core aspects of the recommendation are:

- AT change at start, and periodically during a trip.
- Maximum AT validity period of one week.
- A set of privacy requirements related to AT re-use.
- A recommended solution for AT pool management “Solution C2” and a recommended pool size of at least 60 ATs.
- AT change inhibition in safety related context.

# 2 Introduction

## 2.1 Scope and Purpose of this paper

The purpose of this paper is to present the position of the C2C-CC Consortium on privacy aspects related to V2X communications in European C-ITS Systems and to demonstrate how privacy has been incorporated by design in the standardized security architecture [1].

The scope of the discussion is limited to privacy aspects of V2X broadcast communications as needed for Day 1 applications envisaged by the C-ITS platform [2]. In essence this includes the necessary protection of personal data broadcasted as part of Cooperative Awareness Messages (CAM) [3] and Decentralized Event Notification Messages (DENM) [4].

The scope is limited to the future operation phase of the C-ITS system, with a minimum penetration rate of ITS-Stations in vehicles. The initial ramp-up phase is not discussed.

## 2.2 Why do we need Privacy?

The need for protection and privacy of personal data is sanctioned by the GDPR [5] article 5, which states among other privacy principles: " Personal data shall be: …adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');".

Also note the following definitions (GDPR, Art. 4):

(1)'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(5)'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

(12) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Based on this legal background, the following conclusions are made:

- CAM and DENM contain personal data only if the can be related to an identified or identifiable natural person. In general it does not matter how difficult it is to identify the person, as long as it is technically possible.
- An identifier that uniquely relates to an ITS-Station or an event detected by an ITS-Station in the surrounding area, relates to a vehicle, and hence relates to the driver.
- Single transmitted CAMs and DENMs contain personal data since they are digitally signed and contain an identifier of the signing entity (the ITS-Station's public key certificate), see also the same conclusion by the C-ITS platform [2].
- Traces of CAMs contain personal data in that they are related to location data relevant to an individual, i.e. start and stop position in time of a trip.
- Received CAMs and DENMs can be made anonymous by deleting the references to the transmitting and signing ITS-Station.

- The personal data contained in a CAM is an ITS-Station's four dimensional position, i.e. a position in time and space.
- The personal data contained in a DENM is an event's four dimensional position, i.e. a position in time and space.
- Personal data in CAM and DENM are processed in that they are disclosed by broadcast transmission and can be received / collected and used by other ITS-Stations.

Article 32 states:" the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk,…".

The risk identified is that of the unauthorised disclosure of a vehicle's/person's position in time (independently of the fact of an attacker makes use of the disclosure). The remainder of this paper explains the measures that have been identified to ensure an appropriate level of privacy. Basically, the use of pseudonyms increases the resources that an attacker needs to have to be able to track a vehicle to the same extent [6].

This paper does not address the aspect if and when the processing of personal data contained in CAM and DENM is lawful. It has to be noted that 'Public interest' and 'legitimate interest' seem the most suitable options for legal basis concerning the 'day-one' use cases. Further non-technical aspects of personal data protection such as the transparency principle are also not within the scope of this report.

## 2.3 Privacy towards whom?

This paper considers the risk of unauthorised disclosure of personal data to entities ("privacy attackers") that are able to eavesdrop and decode CAM and DENM broadcasted using ITS-G5 technology. Technically, eavesdropping of ITS-G5 transmission can be performed with appropriate equipment within a radius of 300 to 400 meters.

Long-range spot-check attackers are assumed as an attacker model. This model is characterized in that:

- eavesdropping takes place at some dedicated locations within the system by one or more attackers;
- those locations are at least 1 km distant from each other so that the eavesdropping areas do not cover an entire region;
- the data are shared by the attackers, centrally collected and further analysed to create a "big picture".

It is deemed that ubiquitous eavesdropping, i.e. eavesdropping at locations that are less distant than 1 km and hence covering an entire region is not technically and economically viable.

It is deemed that short-range eavesdropping, i.e. eavesdropping within the range of RF reception of the CAM/DENM does not represent a personal data breach, because: the range is too short to track a vehicle throughout a significant journey (see assumptions in section 4.2); unless the attacker would be following the vehicle, which would correspond to visual tracking and would cause the same breach as without CAM/DENM transmission.

Attackers can further be divided in following categories:

- Outsiders of the C-ITS system, i.e. entities with no further or prior knowledge;
- Insiders of the C-ITS system, i.e. entities that process ITS data, for explicit and legitimate purposes but do further process those data in a manner that is incompatible with those purposes. Those can be further distinguished in:
  - Operators, i.e. entities that operate ITS-Stations
  - Certification Authorities, i.e. entities that have access to certificates issued to ITS-Stations mounted in vehicles.

Aspects of unauthorized disclosure of personal data to manufacturers and/or operators of ITS-Stations are out of scope.

## 2.4 C-ITS performance considerations

The C-ITS system is designed to improve traffic efficiency and traffic safety. The system has been developed during the last 10 years by the C2C-CC among others. This led to a well-established set of standards and profiles. Therefore, it is important to maintain the balance between system performance and high demand on privacy. The following KPIs are important for the performance and reliable operation of the C-ITS system:

- A typical vehicle life span is approximately 15 years. During this life span, the possibility to upgrade the software is very limited. After the vehicle is sold, the manufacturer is not able to replace the hardware.
- Once sold, the manufacturer has limited control over the vehicle. The owner is not required to make use of maintenance and service offers. While in the first three years there is an incentive due to warranty benefits, it is well known that for older vehicles the customer is not willing to invest in maintenance.
- Permanent vehicle connectivity cannot be guaranteed due to limited coverage and high innovation rate in communication technology. It is important to maintain the safety benefit of vehicle to vehicle communication throughout the lifetime of the vehicle. Therefore, the design needs to cope with extended periods of no backend server connectivity.
- The amount of ATs the PKI is able to issue is limited by the backend server capacity. It needs to be guaranteed that vehicle peak usage times (rush hour, holiday) do not create a bottleneck at the PKI. Therefore, servers work load balance is required. As the manufacturer has no control over the vehicle usage, the amount of required ATs needs to be decoupled from the vehicle usage profile.
- The data volume between vehicle and the backend is limited due to transmission costs. Therefore, the amount of ATs must be a trade-off between privacy needs and customer acceptance.
- Customer consent is required for any connectivity.

When designing the measures to protect the privacy of the drivers all these points need to be taken into account. The measures proposed in this paper are a trade-off between the performance of the system and the privacy of the users.

# 3 The conceptual solution: privacy-preserving architecture

## 3.1 General principles

In order to address the risk of a personal data breach due to the transmission and subsequent reception of single CAMs, the C-ITS security architecture standardized by ETSI [1] and adopted by the C-ITS Certificate Policy [7] foresees that CAMs and DENMs are only transmitted in a pseudonymised form, i.e. in a form that cannot be attributed to a data subject with the use of data that is publicly available or available to a single entity. Pseudonymisation means that the CAMs and DENMs include a pseudonym, i.e. and identifier that can only be related to an individual with the collusion of two certification authorities, and only if those certification authorities previously archived information related to the issuing of the certificates to the ITS-Station. This implies that de-facto, there cannot be a data breach neither to outsiders or insiders. Additionally, CAMs and DENMs should be deleted or stripped of the identifiers after reception and processing in order to ensure that they do not contain personal data so to avoid further data breaches to insiders.

If conditions are fulfilled that certification authorities cannot collude and/or do not store data about issued certificates, CAMs and DENMs can be considered to not contain personal data at all. This implies that there cannot be a data breach based on single CAMs and DENMs even to or with the help of certification authorities.

An additional risk that has been identified is that of location linking, i.e. the risk of re-attributing the CAMs to a vehicle/person due to the transmission and subsequent reception of a chain/trace of CAMs during the entire duration of an individual's trip. Therefore, it is planned that the data that would enable the attribution of single positions as a trace to an individual, appropriately changes during the trip, so to prevent the linking of the CAMs. So in order to avoid location linking, the ITS-Station mounted in a vehicle shall change all protocol identifiers in concert and delete unique CAM content such as the trace of last positions. This whitepaper concentrates on changing the reference to the certificate (Authorization Ticket) that can be used to verify the message's signature. This change has to be executed often enough so that CAMs with a same set of identifiers are only eavesdropped at one single attacker's location and an AT change itself is likely not to be observed.

## 3.2 The architecture

The C-ITS security architecture standardized by ETSI [1] and adopted by the C-ITS Certificate Policy [7], requires the issuance of enrolment credentials by the Enrolment Authority and authorisation tickets by the Authorisation Authority to an end-entity, e.g. an ITS-Station mounted in a vehicle.

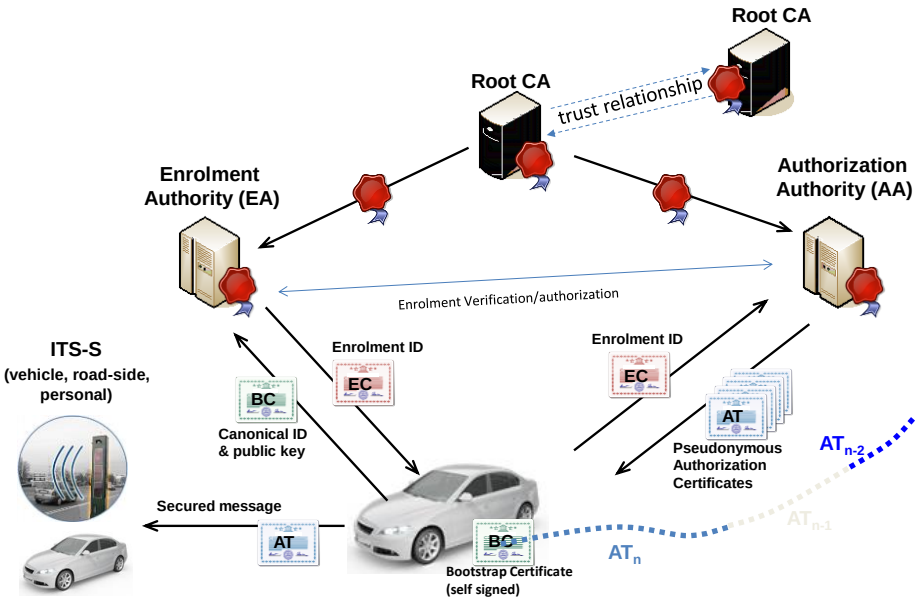


**Figure 3-1: C-ITS security architecture**

Enrolment Credentials provide a static pseudonym to the ITS-Station, that confirms that the ITS-Station is authorized to "be part of the system" and allowed to request authorisation tickets (ATs).

Authorization Tickets (ATs) provide dynamic pseudonyms to the ITS-Station, that confirm that a sender is an authentic ITS-Station and allowed to send certain messages with certain type of content (e.g. CAM or DENM) and can be used to verify the integrity of the message.

The EA and AA shall be separate operational entities, with separate IT infrastructure and separate IT management teams. In order to ensure that using ATs from an AA does not represent a privacy breach, it is assumed that: an ITS-Station request ATs to different AAs so that ATs issued by different AAs are used throughout the same period; that an AA has a customer stock of a minimum size.

Authorization Tickets requests to an Authorization Authority shall be signed using the Enrolment Credential [8], but the signature shall be encrypted so that only the Enrolment Authority can verify the signature against the enrolment credential. In this way, the Authorisation Authority needs to verify each single request with the Enrolment Authority, and single Authorisation Tickets issued upon such request cannot be linked together by the Authorization Authority. On the other hand, the Enrolment Authority is not made aware of which authorization tickets are issued as response to which request.

By virtue of privacy by design build into the architecture, the Enrolment Authority and the Authorisation Authority do not possess a more effective means to obtain personal data from CAM and DENM, than an outside attacker has.

Authorization Tickets used to sign CAMs and DENMs shall be changed regularly in order to avoid location linking. Operational aspects are defined in the next section.

# 4 The operational solution: the practical approach

The conceptual solution provides the framework for protection of personal data. The concept needs to be appropriately instantiated to provide appropriate protection.

## 4.1 AT change strategy

The AT change strategy is based on the paradigm that location linking shall 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 figure below shows and example of separation in three segments, where the first and last segment are typically on lower level roads, and the mid segment is located on higher level roads.


**Figure 4-1: example segmentation. © 2016 Google**

In order to divide trips into those three segments, there are two cases to be considered:

- The end of the trip is known prior to the start of the trip, e.g. because the driver uses a navigation system.
- The end of the trip is not known: this is the default case.

In the first case, the navigation system could most effectively divide the trip into the three segments by changing AT at the correct moment before the end of the trip. Since there is no assurance that the vehicle will be equipped with such a system connected to the ITS-Station and/or the user will always effectively use an on-board navigation system, it was decided to design the system according to the second case. Anyhow it must be noted that for those vehicles equipped with on-board navigation systems (assuming that the user make use of it), an

even increased level of protection of personal data can be assured as with the default second case.

In order to cope with the second case, the last AT change needs to occur before the “always imminent” end of the trip occurs. Since this is not known in advance, it is appropriate to frequently change the AT, to ensure that AT change has occurred recently when the vehicle leaves the mid segment.

Additionally, the frequent AT changes should occur to:

- avoid location linking between two eavesdropping locations, i.e. so that CAMs with a same set of identifiers are only eavesdropped at one single attacker’s location and cannot be observed at a second eavesdropping location. Therefore at least one AT change should happen between two eavesdropping locations and not be observed by an attacker;
- avoid observation of an AT change by the same attacker at the same eavesdropping location. Therefore an AT change should happen between two eavesdropping locations and not be observed by an attacker to prevent linking of ATs.

## 4.2 AT change triggers

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 AT 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:

- An AT change shall 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 AT change shall be performed during the trip randomly in a range of 800 to 1500 meters 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 AT changes shall be performed at least 800 m from the last AT 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 AT can be observed by an attacker at a second location).

Note 1: these values have been obtained using traffic statistics in [10] 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 meters between AT changes makes sure that the same attacker cannot observe an AT change from the same eavesdropping location assuming the “worst” case RF range of 400 meters and the attacker located at the “best” position i.e. 400 meters away from the last change and a trip distance corresponding to RF distance.

Note 3: a change of AT every 800 meters + 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).

For road safety purposes, it is preferable that an AT change is performed when there is a low risk in terms of road safety, e.g. at moments when the vehicle is standing (e.g. at an intersection) or when a low number of neighbouring vehicles is detected. It is also preferable that the AT change time is random, so to avoid easy tracking of the AT change.

## 4.3 AT re-use strategy

### 4.3.1 AT re-use requirements

The re-use of ATs represents a potential weakness in that it would provide the ability for an attacker to re-construct the whereabouts of a vehicle/person, even coarsely throughout different trips. Therefore, two sets of requirements are defined for limiting the risk of a personal data breach: one set of two key performance indicators related to data disclosure in single trips (KPI-1 and 2), and one set of two key performance indicators related to data disclosure throughout multiple trips (KPI-3 and 4).

**The following requirements apply to AT re-use:**

KPI-1. The probability that the AT that has been used for the first segment of a selected trip is re-used for the last segment of the same trip shall be lower than 2%.

KPI-2. The probability that the AT 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 AT that has been used for a mid-segment of a selected trip, is (later on) used for the last segment of the same trip, shall be lower than 20%.

KPI-3. The probability that an AT, 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 shall be lower than 40%.

KPI-4. The probability that an AT, 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) shall be lower than 40%.

Four possible solutions have been identified to address the AT re-use aspect and fulfil the requirements above.

### 4.3.2 AT re-use Solution A

The following conditions apply to AT re-use:

- ATs used for the first segment of a trip shall never have been used before and shall not be used again.
- ATs that have been used for the last segment of a trip shall not be re-used again later. Note that due to the design of the approach, it is not possible to guarantee that an AT that has been used for the last segment of a trip has not been used before.

An implementation shall mark those ATs that have been used in the first or last segment of a trip, i.e. respectively after or immediately before an interruption of a trip. This means that each trip will reduce the number of ATs available in the pool for a specific validity period. It is recommended that the pool shall be refilled if the size drops below a threshold. If the pool is empty, the ITS-Station shall turn in receive mode.

### 4.3.3 AT re-use Solution B

The ATs are drawn from the pool with equal probability and with replacement, i.e. after use they are immediately available for use again.

### 4.3.4 AT re-use Solution C

The ATs are drawn from the pool with equal probability and without replacement, i.e. after use of one AT, that AT is not used again until the pool is re-started. A re-start is done from a new random AT. Re-start can occur in two fashions, therefore the following subvariants are identified:

Solution C1: the pool is re-started after each trip.

Solution C2: the pool is re-started when it is completely empty.

### 4.3.5 AT re-use Solution D

The ATs are drawn from the pool in a sequential round robin fashion, i.e. after using of all ATs in the pool, the ATs are used again in the same order. Re-start is done from a random position in the pool. A re-start can occur in two fashions, therefore the following subvariants are identified:

Solution D1: the pool s re-started after each trip.

Solution D2: the pool is re-started when it is completely empty.

Due to the predictability of the AT change sequence, it is strongly discouraged to use this solution.

## 4.4 AT validity period

In order to limit the long term linkability between segments of trips, **the AT validity period shall be limited to one week**.

Note that from an implementation point of view, not all ATs in the pool of ATs stored in the ITS-Station must have the same validity period. ATs may have different validity periods so that at any point of time a minimum pool size is guaranteed. As an example 50 % of the ATs might have validity Monday to Sunday, whereas the other 50% might have validity Thursday to Wednesday.

The AT preloading period is relevant in that it allows loading ATs in advance of their validity period. Preloaded ATs that are not yet valid, or not valid anymore in a given moment of time are not considered part of the pool at that moment in time. For example, an ITS-Station might have preloaded ATs for January, February and March of a given year. At 12:00 on Wednesday the first of February, only those ATs are part of the pool that are valid at that moment in time.

## 4.5 AT pool size

### 4.5.1 General

The number of ATs that are stored in an ITS-Station and are available for use in a certain moment in time is essentially a trade-off between privacy, cyber-security and technical/economic viability. The pool needs to be big enough to ensure the probabilities established in section 4.3 are reached at every AT selection. On the contrary, a huge pool of ATs would provide the means for a cyber attacker that is able to compromise the ITS-Station to impersonate many vehicles in parallel. Therefore, it is not ideal to have a huge number of ATs stored and valid at the same time. It is to be noted also that it is further recommended to use equipment certified for example according to a Common Criteria Protection Profile to ensure the correct functionality of the ITS-Station and resistance against cyber-attacks.

### 4.5.2 Assumptions

The following assumptions are made considering [10], [12], [13], [14], [15]:

It is assumed that in average a vehicle will be used for 2 trips per day, for 7 days a week; an average trip has length of approx. 15-22 km.

### 4.5.3 Pool size overview

The size of the pool depends on the solution chosen to address the AT change requirements. The pool size is calculated to strictly fulfil the KPIs defined in section 4.3 under the assumptions defined above. An overview is given in the table below. Detailed calculations can be found in 6.

| Column 1 | Solution A | Solution B | Solution C1/D1 | Solution C2/D2 |
|---|---|---|---|---|
| KPI-1 | +28 | 50 | 50 | 50 |
| KPI-2 | 20 | 20 | 20 | 20 |

| Column 1 | Solution A | Solution B | Solution C1/D1 | Solution C2/D2 |
|---|---|---|---|---|
| KPI-3 | +28 | 60 | 60 | 60 |
| KPI-4 | 110 | - | - | - |

**Table 4-1: Pool Size S estimations**

Note: "-" means KPI fulfilled by any pool size

It has to be noted, that at equal pool size S:

- solution C1 achieves in average better KPI results than solution B for KPI-1 and KPI-2;
- solution C2 achieves in average better KPI results than solution B for KPI-1, KPI-2 and KPI-3;

**In conclusion it is recommended to implement solution C2 and to operate a pool of minimum 60 ATs.**

For those drivers that exceed the driving behaviour of the estimated driver profiles, a degradation of the KPI values is expected for those trips that exceed the pool size.

## 4.6 AT change inhibition

In order to support the operation of applications implementing road safety use cases on receiving ITS-Stations, an AT change shall be inhibited by a sending ITS-Station for a maximum defined time of 5 minutes. In fact DENMs can only be correctly reconducted to a single event if they are identified by the same StationId. Therefore, an AT inhibition (along with no change of all other protocol identifiers) shall be supported when DENMs are sent out.

# 5 Appendix 1 – References

## 5.1 List of abbreviations

| | |
|---|---|
| AA | Authorization Authority |
| AT | Authorization Ticket |
| CAM | Cooperative Awareness Message |
| DENM | Decentralized Event Notification Message |
| EA | Enrolment Authority |

## 5.2 Applicable documents


[1] ETSI TS 102 940 V1.2.1 (2016-11) Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management.

[2] http://ec.europa.eu/transport/sites/transport/files/themes/its/doc/c-its-platform-final-report-january-2016.pdf.

[3] ETSI EN 302 637-2 V1.3.2 (2014-11) Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service.

[4] [DENM] ETSI EN 302 637-3 V1.2.2 (2014-11) Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service.

[5] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

[6] Petity, Broekhuis, Feiri, Kargl: Connected Vehicles: Surveillance Threat and Mitigation.

[7] Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS).

[8] ETSI TS 102 941 V1.1.1 (2012-06) Intelligent Transport Systems (ITS); Security; Trust and Privacy Management.

[9] DEPARTMENT OF TRANSPORTATION National Highway Traffic Safety Administration 49 CFR Part 571 [Docket No. NHTSA–2016–0126] RIN 2127–AL55 Federal Motor Vehicle Safety Standards; V2V Communications.

[10] “Deutsches Zentrum für Luft- und Raumfahrt” (German Aeronautics and Space Research Centre - DLR)..

[11] ETSI TR 103 415 (not yet published) Intelligent Transport Systems (ITS); Security; Pre-standardisation study on pseudonym change management.

[12] Statistisches Bundesamt, Wiesbaden - Verkehr in deutschland 2006, https://www.destatis.de/DE/Publikationen/Thematisch/TransportVerkehr/Querschnitt/VerkehrinDeutschlandBlickpunkt1021216069004.pdf?__blob=publicationFile.

[13] Fondazione BNC - La domanda di mobilita' degli Italiani, http://www.isfort.it/sito/statistiche/Congiunturali/Annuali/RA_2011.pdf.

[14] Centraal Bureau voor de Statistiek, Den Haag/Heerlen 3-3-2017, http://statline.cbs.nl/StatWeb/publication/?VW=T&DM=SLNL&PA=71107NED&D1=0&D2=0&D3=0&D4=a&D5=0&D6=a&HD=120229-1025&HDR=T,G5,G4&STB=G1,G2,G3.

[15] Department for Transport - National Travel Survey: England 2014, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/457752/nts2014-01.pdf.

# 6 Appendix 2 – AT change requirements calculations

## 6.1 General

Pool Size is indicated by S

The length of the trip in terms of used AT is indicated by L

The number of trips in a validity period is indicated by T

This implies under the assumptions in section 4.5.2: (L=6; T=14)

## 6.2 Solution A

KPI-1 Calculation:

$p = 0$ By design the probability is zero

The total pool will reduced by at least 28 ATs at the end of the period. This means that the AT pool shall be at least bigger than S+28 certificates per validity period. It is up to the operator of the ITS-Station to decide whether to be on the safe side an upload more ATs for a validity period, or to upload additional ATs “on the fly” if too many of them have been deleted/flagged for non-re-use.

KPI-2 Calculation: “ 1 – probability that last AT is NOT in the mid segment”

$p = \left[1 - \left(1 - \frac{1}{S}\right)^{L-2}\right] < 0{,}20$

Based on the assumptions, a pool size S of at least 20 ATs is needed.

KPI-3 Calculation: “(1-probability that an AT is NOT last in any of the other trips)

$p = 0$ By design the probability is zero

KPI-4 Calculation: (1-probability that AT is NOT in mid segment of any of the other trips)*(probability that AT is not last of any other trip)

$p = \left[1 - \left(1 - \frac{1}{S}\right)^{(L-2)*(T-1)}\right]\left(1 - \frac{1}{S}\right)^{(T-1)} < 0{,}40$

Based on the assumptions, a pool size S of at least 110 ATs is needed.

## 6.3 Solution B

KPI-1 Calculation:

$p = \frac{1}{S} < 0{,}02$

Based on the assumptions, a pool size S of at least 50 ATs is needed.

KPI-2 Calculation: “ (1 – probability that same AT NOT in the mid segment) AND NOT in the first or last segment”:

$p = \left[1 - \left(1 - \frac{1}{S}\right)^{L-2}\right]\left(1 - \frac{1}{S}\right) < 0{,}20$

Based on the assumptions, a pool size S of at least 20 ATs is needed. With a pool size S=60 ATs, this KPI is fulfilled up to L=15

KPI-3 Calculation: “(1-probability that AT is NOT first OR last in any of the other trips)

$$p = \left[1 - \left(1 - \frac{1}{S}\right)^{2*(T-1)}\right] < 0{,}40$$

Based on the assumptions, a pool size S of at least 60 ATs is needed.

KPI-4 Calculation: (1-probability that AT is NOT in mid segment of any of the other trips)*(probability that AT is NOT first OR last of any other trip)

$$p = \left[1 - \left(1 - \frac{1}{S}\right)^{(L-2)*(T-1)}\right]\left(1 - \frac{1}{S}\right)^{2*(T-1)} < 0{,}40$$

This condition is achieved by any pool size.

## 6.4 Solution C1 and D1

KPI-1 Calculation:

$$p = \begin{cases} 0 \;\; if\; L \leq S \\ \frac{1}{S} if\; L > S \end{cases} < 0{,}02$$

Based on the assumptions, the pool size shall be at least 50 ATs. Note that L>S is unlikely to happen according to the assumptions.

KPI-2 Calculation:

$$p = \begin{cases} 0 \;\; if\; L \leq S \\ See\; Solution\; B \;\; if\; L > S \end{cases} < 0{,}20$$

Based on the assumptions, the pool size shall be at least 20 ATs. Note that L>S is unlikely to happen according to the assumptions.

KPI-3 Calculation:

Same as for Solution B

KPI-4 Calculation:

Same as for Solution B

## 6.5 Solution C2 and D2

Let U = the total number of Used ATs since the first start of the pool. Based on the assumptions: U < 100.

KPI-1 Calculation:

$$p = \begin{cases} 0 \;\; if\; a\; trip\; is\; performed\; without\; a\; pool\; re-start \\ \frac{1}{S} \qquad\qquad if a\; trip\; includes\; a\; pool\; re-start \end{cases} < 0{,}02$$

Based on the assumptions, the pool size shall be at least S=50 ATs.

KPI-2 Calculation:

$$p = \begin{cases} 0 & if\; trip\; is\; performed\; without\; pool\; re-start \\ see\; Solution\; B & if\; trip\; includes\; a\; pool\; re-start \end{cases} < 0{,}20$$

Based on the assumptions, the pool size shall be at least S=20 ATs.

KPI-3 Calculation:

$$p = \begin{cases} 0 & if\ U \leq S \\ see\ Solution\ B & if\ U > S \end{cases} < 0{,}40$$

Based on the assumptions, the pool size shall be at least S=60 ATs.

KPI-4 Calculation:

$$p = \begin{cases} 0 & if\ U \leq S \\ see\ Solution\ B & if\ U > S \end{cases} < 0{,}40$$

This condition is achieved by any pool size.

**■ End of Document ■**