



Strategies for changing pseudonyms and sizing the PKI traffic

Deliverable 2.4.4.7

Activity 2: Studies

Sub-activity 2.4 > Specifications

Version 1.00

Publication date: 16/10/2015



Co-financed by the Connecting Europe
Facility of the European Union

Information about the document

Document: Strategies for changing pseudonyms and sizing the PKI traffic

Date of publication: 16/10/2015

Responsible, Entity: Houda LABIOD, Telecom ParisTech

Status: Version 1.00 – Approved

Publication history

Date	Version	Contributeur(s)	Principales modifications	Diffusion
16/10/2015	1.00	Houda Labiod Gérard Segarra J.P. Monteuis Ali Atoui	DIRIF, DIRA Cerema, MTI PSA, Renault	Release 1

Table of Contents

1.	Objective.....	4
2.	State of the art on strategies for changing pseudonyms.....	4
2.1	Fixed Time Change Periodic	4
2.2	Random Change	4
2.3	Silent Period Between Changes.....	4
2.4	Vehicle-Centric Change.....	5
2.5	Density-based Change	5
2.6	Collaborative Change (synchronous)	5
3.	Approach proposed for SCOOP@F.....	6
3.1	Pseudonym changes for ITSS-V	6
3.2	Pseudonym changes for ITSS-V vehicles OBU operator	7
3.3	Pseudonym changes in a pool	7
4.	Sizing.....	8
4.1	Size of keys and certificates	8
4.2	Load related to the PKI in the case of an ITSS-R.....	8
4.3	Load related to the security of CAM messages	9
4.4	Load related to the PKI in the case of an ITSS-C.....	9
5.	Conclusion.....	10
6.	References	11

Table of illustrations

Illustration1: Pool of pseudonym certificates in an ITSS-V OBU operator	7
---	---

1. Objective

The objective of this deliverable is to present the state of the art on strategies for changing pseudonyms in cooperative ITS systems and to describe an approach proposed for the SCOOP@F project. An estimate of the safety traffic, related to the PKI and the CAM messages is delivered in the second part of the deliverable.

2. State of the art on strategies for changing pseudonyms

This section delivers a summary of the main methods proposed in the literature [1].

2.1 Fixed Time Change Periodic

The vehicle periodically changes pseudonym based on a fixed time interval (e.g., every 3 hours). The advantage of this solution is that a vehicle with a pre-loaded pool of pseudonyms can change its pseudonym even if it is outside the range of an ITSS-R. The inconvenience lies in the fact that the pseudonyms are changed based on a fixed time to facilitate tracking. A derivative of this technique called "Time Slotted Pseudonym Pool" involves using a specific pseudonym based on a given time slot (e.g., Noon to 3:00 pm).

2.2 Random Change

The vehicle changes pseudonyms based on a variable time. The advantage of this solution is the difficulty in predicting the moment when the vehicle will change pseudonym. The inconvenience is that the vehicle can easily be detected by tracking solutions if there are few vehicles in its vicinity. Indeed, it may be the only vehicle to change pseudonym at the "tracking" moment. This makes it easily identifiable.

2.3 Silent Period Between Changes

The vehicle stops transmitting during a short period after having changed pseudonym. The interest of this solution is the difficulty, in the context of tracking techniques, of predicting the trajectory of a vehicle after it has ceased transmitting. The limitation of this strategy is that the silence is also applied in the case of security services. This can be highly critical if the vehicle is involved in an accident during the silent period.

2.4 Vehicle-Centric Change

The vehicle changes its pseudonyms independently based on a criterion (e.g., velocity) and then uses a silent period. This approach makes it difficult to track the vehicle since it essentially uses the direction and speed of the vehicle and it is difficult to predict what will be the vehicle's direction and speed after its silent period. The threshold value of the criterion (velocity, etc.) can be fixed based on different parameters (e.g., type of environment (urban zone, rural, etc.)).

2.5 Density-based Change

The vehicle changes its pseudonym when there are N vehicles in its vicinity. This method has the merit of avoiding unnecessary changes of pseudonyms when the vehicle is alone. The value N can be defined based on the environment (rural zone or urban zone). A derivative of this technique is used in the Pseudonyms Synchronously Change (PSC) strategy (see section 2.6).

2.6 Collaborative Change (synchronous)

This strategy uses zones called Mix-Zones in which geo-positioning applications are disabled. These silence zones are located in high traffic areas (hotspots) like a stop light, parking lot or intersection.

We see that there are several possible strategies:

- The vehicle changes pseudonym when it is stopped in the Mix-Zone.
- The vehicles exchange pseudonyms between themselves at their own initiative or through the control of the ITSS-R as described in the S2SI mechanism p3[. This solution makes it possible to place a reduced pool of pseudonyms on board each vehicle.
- The vehicle changes pseudonym at the same time as neighbouring vehicles (Pseudonyms Synchronously Change (PSC)). It is difficult to identify a specific vehicle if all vehicles in the Mix-Zone leave it with a new pseudonym.
-

The pseudonym change strategies have not been tested in the field. Consequently, it is difficult to verify their effectiveness.

3. Approach proposed for SCOOP@F

We describe an initial method that we propose for the SCOOP@F project. It is the result of reflections carried out by Telecom ParisTech and ITS Bretagne. This method is updated in this document to include the recommendations/needs of SCOOP@F participants.

We considered the following hypotheses:

- the pseudonyms of the ITSS-R are long-lasting,
- the pseudonyms of the ITSS-R are short-lasting, and
- these ITSS entities have a pre-loaded pool with a period of validity T .

3.1 Pseudonym changes for ITSS-V

We propose two types of strategy: single and hybrid

3.1.1 Simple strategies

We could envisage the following variants:

- A pseudonym change with a "fixed time change" or "random time change." Each vehicle changes pseudonym on each route and must therefore be able to change it each time the engine starts.
- A pseudonym change triggered after a specified number of uses of the same pseudonym.
- A pseudonym change based on the number of messages sent during a given period. The number of messages is specific to each vehicle. The pseudonym change is harder to foresee. It is easy to identify the vehicle if it changes pseudonym in a zone with few vehicles in the vicinity.
- A pseudonym change every N kilometres travelled. If N is a fixed value, then the pseudonym change strategy become predictable. It is easy to identify the vehicle if it changes pseudonym in a zone with few vehicles in the vicinity.
- A pseudonym change based on kilometres travelled and by speed range. For example, change the pseudonym if the vehicle travels 10 km and the speed is slower than 30 km/h or 50 km travelled and the speed varies between 30 and 80 km/h. The speed ranges can be the same as those defined by the highway code:
 - 0 à 30 km/h: inhabited/hilly urban zones
 - 0 to 50 km/h or 30 to 50km/h: town or fog
 - 50 to 90 km/h: departmental or national trunk road,
 - 90 to 130 km/h: dual carriageways, motorways

3.1.2 Hybrid strategies

The hybrid approach involves combining a simple strategy (among those cited in section 3.1.1) and a strategy from section 2. For example, a hybrid strategy based on the number of messages sent and on the density of vehicles in the vicinity.

3.1.3 Pseudonym changes for ITSS-R

We propose several strategies:

- A pseudonym change with a "fixed time change" or "random time change."
- A pseudonym change triggered after a specified number of uses of the same pseudonym.
- Pseudonym change after receiving N pseudonym requests from vehicles. N can depend on the environment (urban or rural) or can be fixed or random.

The period of validity of pseudonyms has to be defined in order to choose the strategy.

3.2 Pseudonym changes for ITSS-V vehicles OBU operator

We define 2 pools of pseudonyms for the vehicles of road operators:

- 1 business PC pool (PC: Pseudonym certificate),
- 1 road user PC pool

We propose the following strategy: service vehicles change pseudonyms upon arriving at the service activity area. They keep their pseudonyms throughout the duration of their service activity. They change pseudonym again when the vehicle leaves (engine restarts) We consider that on average, for one service activity per day, a service vehicle will need 4 PCs/day (2 PCs/service activity/vehicle). Knowing that a vehicle can have N service activities per day, a vehicle will need $2*N$ pseudonyms for its daily service activities. Furthermore, the pseudonym change is related to the status of the vehicle (e.g., operational status).

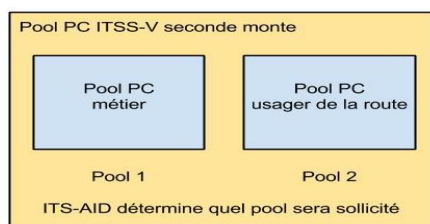


Illustration1: Pool of pseudonym certificates in an ITSS-V OBU operator

If the vehicle is no longer on a service activity, it can switch to a road user vehicle and then the applicable pseudonym change strategy is identical to the one in section 3.1.1.

3.3 Pseudonym changes in a pool

For pseudonym changes in pre-loaded pools in the ITSS-X (X=V/R/vehicle OBU operator), we propose using one of the following techniques: random change or round-robin change. This strategy will be fixed once the size of the pseudonym pools embedded in the ITSS-V (HSM of ITSS-V manufacturer), ITSS-R and ITSS-vehicle OBU operator stations has been defined.

4. Sizing

In this section, we provide an estimate of the load due to safety traffic related to the PKI and CAM messages.

4.1 Size of keys and certificates

Two types of keys are manipulated:

- signature keys generated based on a 32-byte signature algorithm with an elliptical curve (ECDSA NIST p256).
- quantification keys from a 32-byte signature algorithm (ECDSA) of and a 16-byte quantification algorithm (AES 128 CCM).

The ETSI certificates [4] contain a chop of the certificate from the certification authority (8 bytes) and a signature (64 bytes). The total size of all of the components is approximately 150-160 bytes.

4.2 Load related to the PKI in the case of an ITSS-R

4.2.1 Estimation of the number of vehicles in the area of an ITSS-R

The PKI traffic is carried over the G5SC1 channel (equivalent to the SCH1 channel in IEEE 802.11p). The G5SC2 channel (vs. SCH2 in IEEE 802.11p) is not used due to the risk of interferences with the G5CC channel (vs. CCH in IEEE 802.11p). The CAM/DENM messages are sent on the G5CC channel (vs. CCH). 6 10 MHz channels at 6 Mbit/s are available in the 5.850-5.925 GHz bandwidth.

We consider that a CAM message is sent by a vehicle every 100 ms. 10 CAM messages per second are sent by a vehicle, comprised as follows: One approximately 255-byte CAM message with a certificate and 9 approximately 115-byte CAM messages without a certificate.

We assume in our case that the CAM messages are sent every 200 ms (in order not to overload the channel) with a flow of 6 Mbits/s. Therefore, a vehicle sends 5 CAMs ($255 + 4 \times 115$), which equals 5720 bits/s. Then we obtain 1048 vehicles per ITSS-R (without taking into account the "payload" part of the messages).

The PRESERVE project [5] estimated at (IEEE standard 802.11p with a flow of 3 Mbits/s and a transmission frequency of 10 CAM messages/s) 100 the number of vehicles communicating simultaneously.

4.2.2 Load related to the pseudonym traffic

Based on the "Questions and Answers" document and the PRESERVE document [5], we have estimated the traffic generated by the pseudonym requests for an ITSS-V.

We have considered:

- on average 1500¹ PCs are sent per year for an ITSS-V.
- 1 request per PC (we assume that there is a response to each request).

The traffic generated for a PC request is 1 Kb² per PC (request and response).

Knowing that the size of a certificate is approximately 160 bytes for a CA and 125 bytes for the rest (ITSS-V/R).

Therefore, we generate a traffic sized as follows: $1500 \times 1000 \text{ (1kb)} \cong 1.5 \text{ Mb / year / ITSS-V}^3$.

Comments:

- An estimate of the load related to the ITSS-R will be calculated the same way by taking into account a pseudonym change frequency less than that for an ITSS-V.
- We haven't estimated the traffic related to **LTC**, **CRL**, **TSL** related requests because they are negligible compared to the main traffic related to pseudonym changes.

4.3 Load related to the security of CAM messages

We have also estimated the traffic related to CAM messages. We consider that a vehicle travels approximately 2hr/day (in contact with an ITSS-R) and 200 days/year. If an ITSS-V sends 10 CAMs/s (1290 bytes/s) then the total duration in seconds for one year of use is 1,440,000 seconds (200 days x 2hr x 3600s). The CAM traffic generated by an ITSS-V in one year is 1.9 Gb/year. Consequently, we can conclude that the load related to the security of CAM and DENM messages is clearly larger than the load related to the PKI traffic (less than 0.1%).

4.4 Load related to the PKI in the case of an ITSS-C

It is nearly nil.

¹ This value is defined based on the PC change strategy and according to the duration of short and long PCs.

² We could refine the calculation with more precise sizes.

³ This calculation can be adjusted

5. Conclusion

In this deliverable, we propose a group of strategies that can be used. The SCOOP@F project partners can choose one by default and consider certain others as optional.

- For the ITSS-V:
 - A pseudonym change with a fixed or random time change. Each vehicle changes pseudonym on each route and must therefore be able to change it each time the engine starts.
 - A pseudonym change triggered after a specified number of uses of the same pseudonym.
 - A pseudonym change strategy based on the number of kilometres travelled and the vehicle's average speed.
 - A transmission frequency of CAM messages (n Cam/s, n varies based on the congestion status of the channel obtained based on the DCC functionality (Decentralized Congestion Control)),
 - a period of validity of the pseudonym of 2 hours.
- For the ITSS-V OBU operator:
 - a pseudonym change (see section 3.3) that depends on the number of daily service activities to perform,
 - a period of validity of the service pseudonym of 2 hours.
- For the ITSS-R:
 - A pseudonym change with a fixed or random time change.
 - A pseudonym change triggered after a specified number of uses of the same pseudonym.
 - a change strategy based on the number of requests received,
 - a pseudonym period of validity of one year for SCOOP part 1, or even several years for SCOOP part 2.

In order to refine the estimates, we will need:

- the maximum size of the useful part of a CAM message,
- the traffic generated for a pseudonym request (request and response).

6. References

- [1] Petit, J.; Schaub, F.; Feiri, M.; Kargl, F., "Pseudonym Schemes in Vehicular Networks: A Survey," Communications Surveys & Tutorials, IEEE, vol., no.99, August 2014.
- [2] Wang Ying; Yang Shiyong, "Protecting Location Privacy via Synchronously Pseudonym Changing in VANETs," Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on, pp.644-648, 7-9 April 2014.
- [3] Boualouache, A.; Moussaoui, S., "S2SI: A Practical Pseudonym Changing Strategy for Location Privacy in VANETs," Advanced Networking Distributed Systems and Applications (INDS), 2014 International Conference on, pp.70-75, 17-19 June 2014.
- [4] ETSI TS 103 097 (V1.1.15): "Intelligent Transport Systems (ITS); Security; Security header and certificate formats", November 2014.
- [5] PRESERVE - Preparing Secure Vehicle-to-x communication systems – Deliverable 5.2: Deployment issues report v2, 30th January 2013.