A New Approach To Pseudonym Certificate Management in V2X Communication

1st Takahito Yoshizawa
KU Leuven – imec – COSIC
Kasteelpark Arenberg 10 Bus 2452,
B-3001 Leuven, BELGIUM
takahito.yoshizawa@esat.kuleuven.be

2nd Bart Preneel
KU Leuven – imec – COSIC
Kasteelpark Arenberg 10 Bus 2452,
B-3001 Leuven, BELGIUM
bart.preneel@esat.kuleuven.be

***Abstract*—This paper proposes a new solution to the pseudonym certificate management and usage in Vehicle-to-Everything (V2X) communication. This solution is a result of our critical analysis of the Issue First Activate Later (IFAL) pseudonym certificate management scheme, which is mentioned in an ETSI Intelligent Transport System (ITS) pre-standardization document. While the IFAL scheme improves over the existing ETSI ITS Security Credential Management System (CCMS) for Europe and the Security Credential Management System (SCMS) for the US, it still has significant issues when real-world deployment is considered. To address these issues, we propose a novel activation scheme that improves the security properties by combining the OAuth concept and Authentication Encryption with Associated Data (AEAD) solution to provide confidentiality and authenticity of data. Our analysis and simulation show that our scheme significantly improves the security properties and efficiency of certificate usage. As a result, our solution is more robust, reliable, and efficient. We propose this solution for adoption in the ETSI ITS specifications.**

***Index Terms*—V2X, Vehicular Communication, Privacy protection, Pseudonym, Pseudonym Certificate, AES-GCM-SIV**

I. Introduction

V2X communications wirelessly connect vehicles and roadside devices to improve overall road safety. IEEE has published the Wireless Access in Vehicular Environments (WAVE) standard in the 1609 series using IEEE 802.11p as the access layer technology. Since 2015, the 3rd Generation Partnership Project (3GPP) started standardization for V2X communication using mobile technology, called Cellular-V2X (C-V2X). The representative applications are the Dedicated Short Range Communications (DSRC) Basic Safety Message (BSM) [21] in the US, and the Cooperative Awareness Messages (CAM) [7] in Europe.

V2X communications rely on a Public Key Infrastructure (PKI) to protect the security of communications and the privacy of vehicle owners. Broadcast messages such as BSM and CAM require data authentication but do not require confidentiality. It is achieved by digitally signing these messages; the verification of this digital signatures requires the public key of the sender. An authenticated copy of this public key is distributed in a digital certificate issued by a Certification Authority (CA). To protect vehicle owners' privacy, vehicles are required to use pseudonyms and change them periodically along with their associated certificates.

The existing standards for certificate management in V2X communication include SCMS in IEEE 1609.2 [17] in the US, and CCMS in ETSI TS 102 940 [4] in Europe. In addition, IFAL [24] proposes a new approach as stated in the pre-standard report in ETSI TR 103 415 [6]. These schemes achieve the same goal of issuing and delivering certificates to vehicles while using different approaches.

In this paper, we specifically focus on an analysis of IFAL for several reasons. First, it is considered as the leading candidate for ETSI specification [6], [22], [27]. Its approach to separate the distribution and the activation of certificates into two distinct stages has merits over the SCMS [2] and the CCMS schemes [4]. However, a close examination shows that the IFAL scheme has a number of issues, some of which have already been addressed in the SCMS [2]. Second, several key issues in the ETSI's CCMS design [4] are left unresolved. Third, some of its aspects contradict the European Commission's (EC) policy on certificate use [10]. These points motivated us to examine the IFAL design in detail. This paper is our critical analysis on IFAL; we identify its issues, and propose improvements to address them.

The rest of the document is organized as follows. We first discuss related work in Sec II. We then review the existing standards including IFAL in Sec. III, and analyze the IFAL scheme in detail in Sec. IV. In Sec. V and VI, we present a novel solution and evaluate it. Finally, Sec. VII concludes this paper.

II. Related Work

Schmidt [22] summarizes the status of ETSI ITS standard specification, and briefly mentions IFAL as the state-of-the-art certificate management schemes. However, it does not offer a detailed analysis. Other than this, we have identified only one article that analyzes the IFAL scheme in detail, raise issues, and propose an alternative approach to it. Yao et al. [27] proposes an optimized solution called Lightweight Pseudonym Changing (LPC) as an alternative scheme. Its improvement

This work was supported in part by CyberSecurity Research Flanders with reference number VR20192203 and by the Research Council KU Leuven C1 project on Security and Privacy for Cyber-Physical Systems and the Internet of Things with contract number C16/15/058.

over IFAL can be summarized as: (1) introducing both backward and forward secrecy by using a unique *transport key* to encrypt the *activation key* for each *epoch* using a Pseudo-Random Function (PRF) chain, (2) reduction of the storage requirement in the vehicle OBU by issuing ATs per *epoch* basis, (3) ensuring the *activation key* delivery with the use of asynchronous key agreement, and (4) reduction of signature generation time by using a chameleon hash function.

The first and the second points stem from adopting a per-*epoch*-basis AT generation, delivery, and activation. Although it is a valuable proposal, its improvement is limited. In addition, the performance evaluation on the third point indicates mixed results. Moreover, the paper overlooks more fundamental issues that we point out in Sec. IV, e.g. the inflexible AT usage policy (Sec. IV-D). This issue is closely related to the *epoch* concept in IFAL. To resolve it and other issues, our proposed solution removes this concept. In this sense, the level of improvement and impact of our solution is more fundamental than that of [27].

III. Background and Related Standards

A. IEEE 1609.2, 1609.2.1 (SCMS)

The IEEE 1609.2 [17] specifies the certificate management solution for V2X communication in the US, called SCMS [2]. It adopts the pseudonym certificate pool concept proposed by C2C-CC [1] with a minimum of 20 simultaneously active pseudonym certificates. The activation of the certificate is implicit, i.e. vehicles start and stop using certificates based on the validity period in each certificate. This solution [2] allows preloading of up to 3 years worth of pseudonym certificates. For the generation and distribution of certificates, it introduces *butterfly expansion*. This concept allows a vehicle to send one request for which the management system generates multiple pseudonym certificates; it reduces the communication overhead between vehicles and the management system compared to the conventional Certificate Signing Request (CSR). SCMS supports active revocation with the use of a Certificate Revocation List (CRL).

The IEEE 1609.2.1 [18] is another specification that defines detailed operations in end entities, e.g. vehicles, under the SCMS system. For activation of pseudonym certificates, it defines a mechanism called Activation Codes for Pseudonym Certificates (ACPC). It explicitly allows vehicles to operate V2X communication by providing *unlocking values* using binary hash tree as a data structure to convey these values. Although it significantly differs in details with Issue First Activate Later (IFAL) scheme we examine detail in this paper, their objectives and ideas are equivalent – both mechanisms provide a way to convey keys to *unlock* pseudonym certificates in vehicles unless they are revoked. Due the space limitation, we examine exclusively on IFAL in this paper, and plan to analyze ACPC in detail as a follow-up future work.

B. ETSI ITS (CCMS)

In CCMS architecture for Europe, pseudonym certificate is called an Authorization Ticket (AT). For AT generation, TS 102 941 [5] supports both the conventional CSR and the *butterfly expansion* approaches. In the former case, a vehicle generates a private/public key pair and sends the latter to the management system to request a certificate, while the vehicle securely stores the private key, in a tamper-proof Hardware Security Module (HSM).

Unlike SCMS, CCMS does not actively revoke ATs; TS 102 941 [5] specifies the exclusive use of passive revocation where the management system denies future requests by a vehicle to obtain additional ATs if the vehicle has been revoked. This way, as its current ATs expire, a vehicle is excluded from V2X communication.[1]

C. Issue First Activate Later (IFAL)

IFAL [24] is a certificate management scheme proposed for ETSI ITS standardization [6].[2] As the name implies, its main characteristic is a clear separation of generation and loading of ATs to vehicles and the subsequent activation and usage of them. Hence, we discuss the following points in sequence: (1) generation and preloading, (2) activation, and (3) revocation. Time is divided into *epochs*; the IFAL paper proposes its duration of 90 days [24].

1) Generation and Preloading of ATs: A batch of ATs is generated at the time of successful vehicle enrolment with the Enrolment Authority (EA). Preloading of up to 5-year worth of ATs is foreseen. Each AT is assigned to a fixed 12-minute period with 1-minute overlap with the next AT. In other words, only one AT is active at a time, and it is used only once.

2) Activation of ATs: The activation of ATs is done per *epoch*. To do so, the certificate management system sends an *epoch*-specific *activation key* to each vehicle. The derivation of an *epoch key* is illustrated in Fig. 1. An *activation key* for vehicle v for *epoch* i ($K_{ACT_v_i}$) consists of the *epoch key* for vehicle v for *epoch* i ($K_{EP_v_i}$), encrypted by the *transport key* for vehicle v (K_{TR_v}). After decryption of the *activation key*, the vehicle uses the *epoch key* to derive the private key that corresponds to each AT's public key within *epoch* i. Thus, explicit delivery of an *activation key* at each *epoch* allows the vehicle to generate valid signatures for its messages within the *epoch*. In other words, the absence of a valid activation key for an *epoch* prevents the vehicle from generating valid signatures for its messages, effectively revoking a vehicle. The *transport key* is statically fixed for a vehicle at the time of successful enrolment.

3) Revocation of ATs: In IFAL, only passive revocation of ATs is supported. This aligns with both the ETSI ITS specification [5] and the EC's certificate policy [10]. In other words, the management system denies to provide future *activation keys* if the requesting vehicle is identified as revoked.

[1] In this sense, the target of revocation is a vehicle, and not individual certificates. This is a notable point as, in a PKI context, certificates are revoked rather than the entity that use them.

[2] Its original version appeared in 2016. In this paper, we reference and analyze the latest version published in 2019 [24].

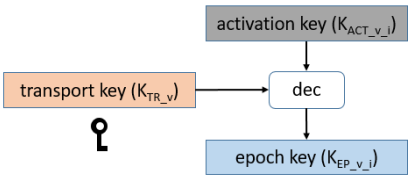

Fig. 1. Epoch Key Derivation in IFAL

IV. IFAL Issues

A. Wasted Certificates

The IFAL's approach to generate ATs is highly inefficient as it does not take the actual vehicle usage into account. Typically, passenger vehicles are driven no more than a few hours a day, e.g. daily commuting. Studies show that the average daily commute times in Europe is 46.1 minutes per day for employees [14]; in the US, it is 27.6 minutes one-way (55.2 minutes round trip) [3]. Under the IFAL scheme, this translates to not using 95.2% of the generated ATs for employees in Europe, which represents a significant amount of unneeded computation, distribution, and storage of certificates.

According to the latest statistics, the total number of vehicles in EU countries is approximately 277.8 million [8]. If the IFAL scheme were deployed in all vehicles in all EU countries, $\sim$13.27 trillion (13.27×10^{12}) ATs, or $\sim$1.95 petabytes (1.95×10^{15} bytes) of ATs would require storage and transmission per year. Out of these, $\sim$1.85 petabytes of data, are discarded without being used. This waste of energy is also undesirable from an environmental impact perspective.

B. Transfer of Private Key Information over Activation

As discussed in Sec. III-C2, in the IFAL scheme, the vehicle receives *activation key* per *epoch* and derives *private keys* to sign messages. In other words, the information to derive private keys is transmitted to the vehicle during the activation process. This is in contrast to the conventional CSR process where the entity that requests a certificate generates and securely stores the private key. If an adversary successfully breaks this *transport key*, all private keys that correspond to all ATs in the *epochs* for the specific vehicle are revealed. This opens an opportunity to compromise vehicles' operation.

C. No Forward and Backward Secrecy

The issue discussed in Sec. IV-B further implies that the IFAL scheme fails to guarantee both *forward* and *backward secrecy*. The *transport key* is generated during the initial vehicle enrolment with the EA. As the IFAL scheme does not renew this *transport key*, it is static per vehicle once it is generated. This has a significant implication – if an adversary breaks a vehicle's *transport key*, all private keys that correspond to all ATs in all past, present, and future *epochs* for this vehicle are revealed. This adversary can generate valid signatures for all ATs within the current and future *epochs* by obtaining current and future *epoch keys* by decrypting *activation keys*. Therefore, the IFAL scheme offers neither *forward* nor *backward secrecy*. Further, it offers no solution to recover from this situation due to the absence of a mechanism to re-key the *transport key*.

D. Inflexible AT Usage Policy

The AT usage in the IFAL scheme is one-time only in a strictly sequential manner with each AT valid for a specific 12-minute interval. This regular and periodic time-based AT change behavior may allow observers to link ATs, hence compromising the unlinkability property. From the perspective of maintaining unlinkability, it is better to introduce variability or randomness in change intervals.

E. Gap Period in Passive Revocation

The IFAL scheme adopts only passive revocation for ATs (Sec. III-C3). This creates its own issue – it leaves a time gap between the time when a vehicle is revoked and when the vehicle stops transmission. As discussed in Sec. III-C2, an *activation key* is delivered to a vehicle per *epoch* of 90 days. This implies that a revocation event of a vehicle will not stop the vehicle from transmitting messages until the end of the current *epoch*. In the worst-case scenario, this time gap is as long as the *epoch* duration, i.e. 90 days. This implies that the *epoch* duration significantly influences the timeliness of the revocation. The shorter the *epoch* duration, the better from a revocation perspective. However, it comes at the cost of more frequent *activation key* distribution. There is a clear trade-off between the revocation timeliness and the activation frequency. The same issue applies to the ETSI standard as it relies on passive revocation only [5]. In this case, a vehicle becomes aware of its revoked condition when the Authorization Authority (AA) denies the next AT request from the vehicle.

F. Sub-optimal and Unreliable Activation Channels

The IFAL scheme [24] uses SMS and manual operation as activation mechanisms. However, it does not address potential situations where SMS messages are not delivered, nor does it address recovery mechanisms from such conditions.

The IFAL paper [24] justifies the use of SMS given the mandate of EU eCall directive in 2018 [11]. This directive clarifies that the in-vehicle mobile terminal stays dormant unless an accident occurs [11], [20]. This statement implies that the vehicle's mobile device is not registered to the mobile network under normal circumstance; thus SMS messages cannot be delivered to it. In addition, there are well-known security vulnerabilities in SMS as multiple ways exist to circumvent SMS-based multi-factor authentication (MFA) [15], [23]. As a result, the US National Institute of Standards and Technology (NIST) recommends to not use SMS-based MFA.

V. A Novel Activation Scheme

A. Goals and Assumptions

The goals we aim to achieve include addressing all issues we identified in Sec. IV. In addition, we include the following elements into the solution design: (1) automatic activation

without human intervention, (2) detection and recovery from failure conditions, and (3) taking usage scenarios into account where vehicles may not be driven every day.

As security assumptions, we consider that the HSM can be potentially malicious, thus can possibly disrupt the activation procedure by launching active attacks such as replay attack or intentionally causing the procedure to fail. A fake HSM may attempt to impersonate another vehicle's HSM to create a DoS type situation to a victim vehicle. In addition, there can be adversaries that may passively monitor the communication between the HSM and the management system to obtain information that identifies vehicles or compromise vehicle owners' privacy. We take our design by taking these points into consideration.

B. Solution Description

Our solution combines existing concepts in a novel manner to address the issues identified in Sec. IV and goals stated in Sec. V-A. We introduce a different approach to the activation; activation serves as a mean for the management system to periodically and explicitly give permission to the vehicle to transmit V2X messages. For this purpose, we combine the OAuth model [16] and the use of a user's device (remote key) as means of authorization. Involving a user's device for authorization aligns with the trend in MFA solutions to be applied in V2X context [19].

The OAuth model views the signature generation as a service that the HSM provides to the OBU. This way, our solution realizes the equivalent end result of revoking the vehicle's ATs by the HSM denying its service. Figure 2 illustrates the overall concept and the mapping of OAuth entities to the vehicle context. In OAuth terminology, the *resource owner* is the user (e.g. driver); the *client* or the *user agent* is the vehicle's On-Board Unit (OBU); the *resource server* is the vehicle's HSM; the *authorization server* is the AA in the certificate management system, respectively.

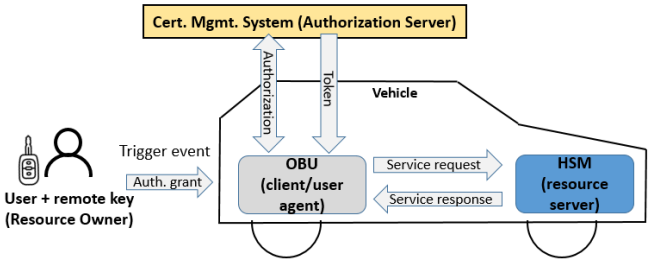

Fig. 2. OAuth Model in Vehicle Context

We use a modified version of the OAuth framework for the activation procedure. The procedure is triggered by the user unlocking the vehicle's door using the remote key and starting the engine. This user's action is considered as an implicit authorization to the vehicle OBU (*user agent*). This event triggers the OBU to initiate the HSM (*resource server*) to query its *activation status* to the AA (*authorization server*). Then the AA checks the revocation status of the vehicle and returns it to the HSM as the *activation status*.[3] Upon receipt, the HSM reflects this status to its operation: whether to enable or disable signature generation for messages that the OBU generates. Finally, the HSM returns an acknowledgment to the AA.

C. Detailed Description – Activation

We use AES Galois/Counter Mode Synthetic Initialization Vector (AES-GCM-SIV) specified in RFC 8452 [13] as a building block of the mechanism to generate, deliver, and verify the vehicle's *activation status*. AES-GCM-SIV is a type of Authentication Encryption with Associated Data (AEAD) which assures both confidentiality and authenticity of data. AES-GCM-SIV has been integrated in Google's BoringSSL library and in QUIC [12]. It is designed to be resistant to potential reuse of nonce when its uniqueness is not guaranteed. It uses a vehicle-specific key generation key (KGK, $k_{KG_v,i}$) to derive a pair of keys for encryption ($K_{enc,i}$) and authentication ($K_{auth,i}$) for each nonce. In addition, we also re-key this KGK at every iteration (i) of this procedure. This dynamic update of KGK is the main difference in our solution while the *transport key* remains static in the IFAL scheme.

Figure 3 illustrates the processing in both the AA and the HSM according to RFC 8452 [13].[4] This procedure is strictly between the AA and the HSM; the vehicle OBU is simply a pass-through. Table I shows the notations.

TABLE I
NOTATION DEFINITIONS

Notation	Definition
AD	additional data
$AEAD$	Authentication Encryption with Associated Data
$H()$	hash function
$k_{KG_v,i}$	key generation key for vehicle v for iteration i
$k_{enc,i}$	encryption key (per RFC 8452) for iteration i
$k_{auth,i}$	authentication key (per RFC 8452) for iteration i
k_{AApub}	public key in AA's server certificate [5]
k_{AApri}	private key of AA [5]
KDF()	Key Derivation Function
$LTcertID_v$	long-term certificate ID of vehicle v
R	random value

First, the HSM generates a random value (R) and concatenates it with the vehicle-specific long-term enrolment certificate ID ($LTcertID_v$)[5] to generate the associated data (AD), and sends it to the AA in ActivationStatusQuery message (Step 1 in Fig. 3). This message is encrypted using the public key in the AA's server certificate (k_{AApub}) as defined in TS 102 941 [5] to conceal signaling messages. The AA first decrypts this message using the corresponding private key (k_{AApub}) and runs the authorization validation with the EA, as defined in

[3] An *activation status* is semantically equivalent to an activation key in the IFAL scheme.

[4] RFC 8452 [13] defines detailed building blocks and operations such as POLYVAL, padding, and truncation. However, in this figure, we restrict ourselves to the description at a high-level abstraction that is sufficient to understand the scheme.

[5] This $LTcertID_v$ is issued by the EA at the time of the vehicle's successful enrolment. Thus, HSM's possession of it is a pre-condition. As a part of our solution, we also require that this ID is stored in the tamper-resistant HSM.

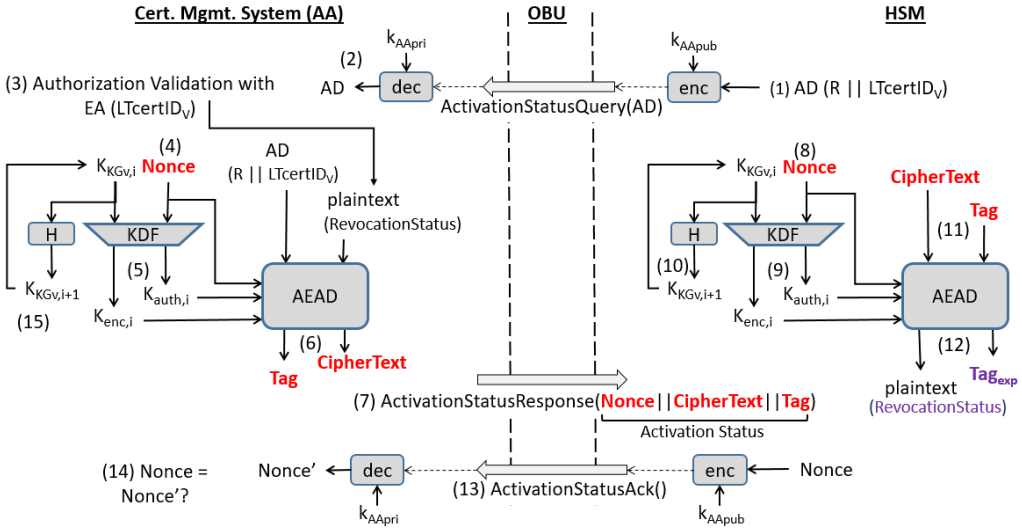

Fig. 3. Activation Status Generation and Verification

[5], to check the requesting vehicle's revocation status using the received $LTcertID_v$, and reflects this status to the plaintext (Step 2, 3). Next, the AA generates a nonce and, along with the current KGK, creates a key pair $(K_{enc,i}, K_{auth,i})$ (Step 4, 5). Using inputs of a tuple (plaintext, *AD*, nonce, $K_{enc,i}$, $K_{auth,i}$), the AA generates a tag and a $ciphertext$ [13] (Step 6). Finally, the AA encrypts the concatenation of ($nonce$, $ciphertext$, tag) using k_{AApri} and send its output to the HSM as the *activation status* in the ActivationStatusResponse message (Step 7).

The receiving side follows the reverse operation to obtain the plaintext and verify its authenticity. Upon receiving this response message, the HSM decrypts it using k_{AApub}, extracts the nonce, and follows the same procedure to derive $K_{enc,i}$, $K_{auth,i}$, and $k_{KG_v,i+1}$ (Steps 8–9). It also derives the next KGK ($k_{KG_v,i+1}$) using a cryptographic hash function (Step 10). Then it decrypts the ciphertext to obtain the plaintext and generates the expected tag (Tag_{exp}), and verifies if the received tag and the expected tag match (Step 11, 12). If they match, the HSM reflects the received revocation status to the operation of signature generation function, i.e. if this status indicates the vehicle is revoked, the HSM disables its signature generation function; otherwise, it enables this function.

Finally, the HSM encrypts $nonce$ and sends its output as an ActivationStatusAck message to the AA (Step 13). The AA decrypts it using k_{AApri} to obtain $nonce'$ and verify if $nonce = nonce'$ holds (Step 14). If so, the AA updates $k_{KG_v,i+1}$ (Step 15). This final step ensures the AA that the HSM has successfully received the activation status and updated the KGK. This three-way handshake prevents the KGK mismatch condition, which may be caused by an error event, e.g. a temporary communication failure. Further, if this procedure fails, the HSM may retry the procedure as a recovery action. At the end of a day (or a 24-hour cycle since the last successful activation), the HSM resets its state so that it requires a new activation to continue the normal signature generation and this activation procedure is repeated.

D. Detailed Description – OBU Tx Operation

When the OBU constructs a new V2X message, it requests the HSM to generate a signature by passing a message digest d. If the activation is successful, according to the procedure in Sec. V-C, the HSM generates a valid ECDSA signature (r, s) to the message and returns it to the OBU; the OBU then transmits the message. If the activation is unsuccessful, then the HSM ignores the OBU's request to generate a signature, which triggers a time-out event at the OBU; thus it is not able to transmit the message.

E. Detailed Description – Certificate Use

In our solution, we observe the EC recommendation in which the maximum preloading period of ATs is 3 months [10]. It reduces the AT storage requirement in vehicles compared to longer period, e.g. 5 years as proposed in the IFAL scheme [24]. Each AT is assigned to a longer period by *floating* them within the intended usage period, e.g. a period of a week. This is the approach proposed by C2C-CC [1] (Sec. III-A), and has a benefit of reducing waste of unused ATs (Sec. IV-A).

VI. Analysis and Discussion

A. Security Properties

We now analyze the security properties of our solution described in Sec. V. Based on the security assumptions in Sec. V-A, we analyze our solution based on the following types of attacks: (1) replay attack, (2) impersonation attack, (3) intentional procedure failure, (4) suppressing the activation procedure, and (5) passive observation to obtain privary information. In addition, we also consider the scenario to cause the KGK misalignment.

First, to prevent replay attack, our procedure uses two unique numbers in each execution of this procedure to prevent

this type of attack; one is R generated by the HSM and $nonce$ used by the AA. Specifically, the HSM sending the $nonce$ value received in ActivationStatusResponse message (Step 7) in ActivationStatusAck message (Step 14) prevents this type of attack by a fake HSM.

Second, impersonation as another vehicle is mitigated as the attacker requires the *LTcertID*$_v$ for this purpose. This value is delivered to the vehicle at the time of successful enrolment with the management system, implying that only the legitimate vehicles possess this value, and it is unique to each vehicle. As this ID is stored in the vehicle's tamper-resistant HSM, impersonation attack requires successfully breaking into the HSM module, which goes against the fundamental security tenet described in TS 102 940 [4].

Third, intentional procedure failure situations can be caused by a compromised or a fake HSM. As stated above, resistance against tampering of HSM is a fundamental tenet of the V2X certificate management system [4]. Therefore, the HSM's use of the *LTcertID*$_v$ in the procedure and the corresponding verification in the AA will prove the HSM's legitimacy.

Fourth, a compromised vehicle may suppress this activation procedure. However, our solution sets an expectation in the AA that each vehicle executes this procedure periodically, e.g. daily. This way, an absence of this activation triggers the AA to suspect a malicious vehicle. At the same time, a daily execution of this procedure is not guaranteed in reality as vehicles are not necessarily driven every day. Furthermore, temporary unavailability of communication with the management system at the time of vehicle use results in the similar situation. To address this variability, the management system can configure a maximum time interval to the vehicle as a system parameter. At every successful activation, the AA resets this timer. From the AA's perspective, the absence of this procedure longer than this interval can indicate that a vehicle is potentially malicious.

Fifth, our solution prevents passive observers from compromising vehicle owner's privacy. The only potential information that may lead to privacy in the activation procedure is *LTcertID*$_v$ in the ActivationStatusQuery message. However, obtaining this information requires successfully decrypting this message which require k_{AApri} that is secretly stored in the AA. This implies an adversary needs to successfully break into the AA to steal this private key. This is clearly beyond the scope of passive observation.

Finally, update of KGK ($k_{KG_v,i+1}$) requires careful consideration as its misalignment will cause future execution of this procedure to fail. For example, a fake ActivationStatusAck message by a fake HSM sent at the right timing can create this situation as the AA updates its KGK but the real HSM may not. In this respect, the three-way handshake described in Sec. V-C requires the AA to verify this ack message is a valid one. In our solution, we ensure this condition by the HSM re-sending R that was sent in the earlier step of the procedure. However, this time, R value is encrypted without other information, unlike AD as shown in the first message in Fig. 3. As these messages are encrypted, this makes it difficult for passive eavesdroppers to correlate or identify this value. Verifying the R value in the first message against the one obtained in the ActivationStatusAck message ensures that this message is sent by the same entity that started the procedure.

B. Storage and Bandwidth Comparison

Table II summarizes the quantitative analysis of IFAL and our solution. From storage capacity perspective, the IFAL scheme requires over 1.5 Mbytes in a vehicle to store 3 months amount of ATs while our scheme requires 34 Kbytes for the same period, i.e. $\sim$2.2% of the former. Furthermore, if we follow the IFAL scheme [24] in which vehicles are preloaded for 5-year worth of ATs, the vehicle's storage requirement exceeds 31.5 Mbytes, while our scheme requires less than 700 Mbytes. Furthermore, our scheme reloads ATs on a weekly basis after the initial preloading period of EC-recommended 3 months ends [10]. This means that the storage requirement in vehicles will reduce from 3 months to one week worth of ATs, which is merely $\sim$2.6 Kbytes.

Next, we consider the bandwidth usage required to transfer ATs to vehicles. For this comparison, we base our traffic calculation at the certificate management system rather than at the vehicle to avoid possible variations of communicate path, such as wide-area mobile network or V2I connection to Road Side Units (RSU).[6] Given that the signaling messages in our solution (ActivationStatusQuery, ActivationStatusResponse, and ActivationStatusResponse) are newly introduced messages, we use the message lengths of Authorization Request and Response messages defined in [5] as the baseline for comparison. The *activationCode* message as described in [24] is sent to vehicles per epoch (90 days).

C. Simulation Result of AES-GCM-SIV

We conducted a simulation to evaluate the performance of our AES-GCM-SIV-based activation solution. It was run on a pair of PCs, equipped with Intel i7-6600U dual-core CPU at 2.6 GHz with 32GB of RAM running Windows 10, and the AES-GCM-SIV is based on an implementation in [26]. We corrected several bugs in this code, and added a communication functionality. We executed three sets of simulation run with varying amount of delays in the response message: (1) no delay, (2) 10 msec, and (3) 15 msec, respectively. These intentional delays are inserted at the server side to simulate the database query and communication latency. For each case, we executed 2000 message exchanges and took an average. The resulting performance numbers are shown in Table III.

We describe the performance in terms of the number of activation procedures per second as it provides indication of how much processing capacity the management system needs in order to account for the number of queries the system receives from vehicles. With no delay in response (case 1), one procedure run takes slightly over 5 msec, which translates to

[6]The MTU of Ethernet frame and IPv6 packet are 1500 and 1280 bytes, respectively. We also account for the extra IPv6 headers for fragmentation. Additionally, TS 102 941 [5] specifies that the security management-related messages are encrypted using the respective server certificates; therefore, we assume that generic security protocols such as Transport Layer Security (TLS) is not used for the protection of signaling messages.

TABLE II
COMPARISON OF REQUIRED STORAGE AND BANDWIDTH

Content	Size (bytes)	
	IFAL	Our solution
Storage Capacity Requirement		
# of certs, 1 week	916[1]	20[1]
Cert size, 1 week	120,960	2,640
# of certs, 3 months	11,782[1]	257[1]
Cert size, 3 months	1,555,200	33,943
# of certs, 5 years	238,909[1]	5,214[1]
Cert size, 5 years	31,536,000	688,286
Effective storage required	31,536,000	33,943
Bandwidth Usage Requirement		
Message headers (Eth/IPv6/TCP)	94	94
ActivationStatusQuery message	n/a	258
ActivationStatusResponse message	n/a	149
ActivationStatusAck message	n/a	149
Single cert. req/resp	n/a	595
Batch cert. req/resp	n/a	11,900
ActivationCode message	149	n/a
5-year cert. download	33,413,481	3,102,500[2]

Note 1: The unit is number of certificates (all others are bytes).
Note 2: This number is shown strictly for comparison purpose only as our solution support maximum of 3-month worth of ATs.

TABLE III
SIMULATION RESULT OF AUTHORIZATION QUERY / RESPONSE

Case	Avg. Request /Response Time (sec)	Avg # of Requests/sec	Condition
1	0.005231	196.803	no delay
2	0.015935	63.086	10 msec delay
3	0.021882	46.102	15 msec delay

196 interactions per second. With 10 msec and 15 msec delay (case 2, 3), the number of procedures per second reduces to 63 and 46, respectively.

Forty-six queries/sec. with 15 msec delay translates to 165,600 queries/hr. As an estimate, we use the statistics of Germany [9] given that it has the largest number of registered vehicles and population in Western Europe (48.427 million registered vehicles for the population of 83.3 million (58.14%)). The most populated state is North Rhine-Westphalia which has 17.926 million people [25]; it translates to 10.421 million registered vehicles according to this vehicle/population ratio. If all of these vehicles issues one query per day, then it translates to 434,215 queries/hr. Our simulation result indicates that 3 servers of this performance will suffice to serve all queries for the vehicle population. This simulation result indicates that applying our solution is a viable one.

D. Advantages

Table IV summarizes the advantages and disadvantages of our solution. Our solution has a number of advantages over both the IFAL scheme and the CCMS in the ETSI ITS standard, and addresses all issues we identified in Sec. IV. As a result, it has a higher level of security and is more robust than the IFAL scheme for the following reasons.

Our solution significantly shortens the latency to evict misbehaving vehicles due to the change of the semantics of *activation* on a daily basis. Thus, a negative outcome of the activation procedure immediately stops the vehicle's transmission by denying the HSM from generating valid signatures. Furthermore, our solution minimizes the inefficient use of ATs and alleviates the vehicle storage due to the combination of longer validity period to ATs (e.g. a week) and following the EC recommended preloading period of 3 months [10]. The exact AT usage is delegated to vehicles based on the actual driving and usage, rather than being dictated by the inflexible validity period set in ATs. Activation occurs automatically without user intervention, triggered by the user's remote key to unlock the vehicle door and start the engine. The solution also mitigates failure conditions by retrying the procedure.

Deploying our solution requires implementations only in the vehicle HSM and the AA; no other system entities are impacted as the solution is transparent to them. A software-only solution incurs no hardware retrofitting or replacement. Finally, our solution accounts for realistic vehicle usage scenarios where a vehicle may not be driven every day.

E. Disadvantages

Our proposed scheme includes a few downsides compared to the IFAL scheme. However, they are relatively minor and can be mitigated. The first is concerning the shorter activation period; a more frequent activation increases the processing in vehicles and the management system and network traffic between them. However, as shown in Sec. VI-B, activation procedure consisting of three messages requires a small amount of data ($\sim$550 bytes) only. In addition, as the *connected vehicle* usage (e.g. infotainment) increases, the short daily activation procedure will be a negligible increase with respect to the total data volume a vehicle generates in a day.

The second downside is the nature of the CSR-based AT request. It is supported in the ETSI ITS standard along with the *butterfly key expansion* scheme [4]. Although the latter is more efficient in terms of generating an arbitrary number of ATs in a single request, it requires transferring the activation key for the vehicle to dynamically generate private keys from it. However, this scheme does not suit well to our solution due to the change of *activation* semantics. This situation implies that the vehicle requires repeating the AT request procedure n times to obtain n ATs during the preloading period, which is less scalable than the *butterfly key expansion* scheme. However, as the number of ATs simultaneously active is rather limited ($\sim$20 ATs per week according to C2C-CC [1]), this situation is considered as a trade-off of all advantages our solution offers.

VII. CONCLUSION AND FUTURE WORK

In this paper, we introduced a novel solution for pseudonym certificate management. Our solution combines OAuth concept and an efficient AEAD scheme (AES-GCM-SIV) along with modified activation semantics. It addresses all identified issues from our close examination of the IFAL scheme. Our analysis and simulation result show that our solution improves in security property, communication volume, and storage requirement perspectives. The issues we identified in the IFAL scheme and thus addressed in our solution are significant to an extent

TABLE IV
COMPARISON OF KEY POINTS IN SOLUTIONS

Characteristics	IFAL Solution	Our Solution
Advantages of Our Solution		
Key in activation, freshness, forward & backward secrecy	Static transport key, re-key not supported, Forward and backward secrecy not supported.	Use of random and nonce, KGK key pair and re-key at every activation. Forward and backward secrecy are maintained.
Activation key derivation, key encryption	SMS or manual operation, using asymmetric encryption, potential key leakage.	AEAD-based (AES) solution over control channel, implicit re-key prevents leakage.
Private key derivation	Seed info (*activation key*) sent at activation.	Securely stored in the vehicle's HSM.
Passive revocation time gap	Max. of 1 *epoch* long (90 days).	Max. of 1 activation cycle (e.g. 1 day).
Activation interval	Per-*epoch*-based (90 days).	Shorter (daily) activation, remove *epoch* concept.
AT preloading & storage	5-year worth of ATs.	Max. 3-month worth of ATs.
AT usage & waste	Fixed 12-min period, large waste.	Vehicle-centric flexible usage policy.
Activation trigger	SMS or manual operation.	User's action to use the remote key.
Activation failure handling	Not addressed.	Failure detection and retry.
Disadvantages of Our Solution		
Activation cycle	Per-*epoch*-based (90 days).	Shorter (daily) activation.
AT generation	5-year worth of ATs preloaded before activation.	CSR approach needs scalability improvement.

that the former introduces negative impacts in various aspects, including lack of robustness as a security solution as well as its environmental impact due to its highly inefficient use of certificates. We propose that our new enhanced scheme is considered for adoption in the ETSI ITS standard. As our future work, we plan to investigate further improvements in the use of CSR in our solution. In addition, detail analysis of ACPC in IEEE 1609.2.1 as discussed in Sec III-A and performance comparison of our solution against it is our next step.

REFERENCES

[1] N. Bißmeyer, H. Stübing, E. Schoch, S. Götz, J. P. Stotz, and B. Lonc, "A Generic Public Key Infrastructure for Securing Car-to-C Communication," 18th ITS World Congress, Orlando, USA, Vol.14, 2011.

[2] B. Brecht, T. Hehn, A. Weimerskirch, W. Whyte, V. Kumar, T. Hehn, and R. Goudy, "A Security Credential Management System for V2X Communications," IEEE Transactions on Intelligent Transportation Systems, Vol. 19, No. 12, pp. 3850–3871, Dec. 2018.

[3] C. Burd, M. Burrows, B. McKenzie, "Travel time to work in the united states: 2019," American Community Survey Reports, United States Census Bureau, 2021

[4] European Telecommunication Standard Institute (ETSI), "TS 102 940 Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management, Ver.2.1.1," July 2021.

[5] European Telecommunication Standard Institute (ETSI), "TS 102 941 Intelligent Transport Systems (ITS); Security; Trust and Privacy Management, Ver.2.1.1," Oct. 2021.

[6] European Telecommunication Standard Institute (ETSI), "TR 103 415 Intelligent Transport Systems (ITS); Security; Pre-standardization study on pseudonym change management, Ver.1.1.1," Apr. 2018.

[7] European Telecommunication Standard Institute (ETSI), "EN 302 637-2 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service," Ver.1.4.1, Apr. 2019.

[8] European Automobile Manufacturers Association, "ACEA Report Vehicles in use Europe," Jan. 2021 [Online]. Available: https://www.acea.auto/files/report-vehicles-in-use-europe-january-2021-1.pdf

[9] CEIC Data, "Germany," [Online]. Available: https://www.ceicdata.com/en/country/germany

[10] European Commission, "Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)," Release 1.1, June 2018

[11] European Commission, "Mobility and Transport," [Online]. Available: https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en

[12] S. Gueron, A. Langley, and Y. Lindell, "AES-GCM-SIV: Specification and Analysis," *Cryptology ePrint Archive, Report 2017/168*, [Online]. Available: https://ia.cr/2017/168

[13] S. Gueron, A. Langley, and Y. Lindell, RFC 8452, "AES-GCM-SIV: Nonce Misuse-Resistant Authenticated Encryption", Internet Research Task Force (IRTF), April 2019

[14] J. I. Giménez-Nadal, J. A. Molina, and J. Velilla, "Commuting and self-employment in Western Europe," Journal of Transport Geography, Elsevier, vol. 88, p.102856, 2020

[15] R. Grimes, "The many ways to hack 2FA," Network Security, Elsevier, vol. 2019, no. 9, pp. 8–13, 2019 =

[16] D. Hardt, "RFC 6749: The OAuth 2.0 authorization framework," Internet Engineering Task Force (IETF), 2012

[17] IEEE Vehicular Technology Society, "IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages," IEEE Std 1609.2-2016, 2016

[18] IEEE Vehicular Technology Society, "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) — Certificate Management Interfaces for End Entities", IEEE Std 1609.2.1-2022, 2022

[19] A. Ometov, S. Bezzateev, "Multi-factor authentication: A survey and Challenges in V2X Applications," 9th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), pp. 129–136, IEEE, 2017

[20] R. Oorni, and A. Goulart, "In-vehicle emergency call services: eCall and beyond," IEEE Communications Magazine, vol. 55, no. 1, pp. 159–165, 2017

[21] SAE International, "J2735 Dedicated Short Range Communications (DSRC) message set dictionary," SAE International Standard, 2009.

[22] O. Schmidt, "An ETSI look at the State of the Art of pseudonym schemes in Vehicle-to-Everything (V2X) communication," [Online], July. 2018. Available: https://git.orlives.de/schmittlauch/hs-pseudonym-schemes-in-v2x/src/branch/master/main.pdf

[23] S.W.A. Shah, J.J. Jeong, and R. Doss, "How hackers can use message mirroring apps to see all your SMS texts — and bypass 2FA security," [Online]. Available: https://theconversation.com/how-hackers-can-use-message-mirroring-apps-to-see-all-your-sms-texts-and-bypass-2fa-security-165817

[24] E. Verheul, C. Hicks, and F. D. Garcia, "IFAL: Issue first activate later certificates for V2X," IEEE European Symposium on Security and Privacy (EuroS&P), pp. 279–293, 2019.

[25] "States of Germany," [Online]. Available: https://en.wikipedia.org/wiki/States_of_Germany

[26] "aes-gcm-siv," Oct. 18, 2016 [Online]. Available: https://github.com/chris-wood/aes-gcm-siv

[27] Y. Yao, X. Chang, J. Wang, J. Mišić, V.B. Mišić, H. Wang, "LPC: A Lightweight Pseudonym Changing Scheme with Robust Forward and Backward Secrecy for V2X," Ad Hoc Networks, Elsevier, p. 102695, 2021