Journal of
Sensor and Actuator Networks

MDPI

Article

Efficient and Privacy-Preserving Certificate Activation for V2X Pseudonym Certificate Revocation

Jan Wantoro [1,*] and Masahiro Mambo [2]

[1] Division of Electrical Engineering and Computer Science, Graduate School of Natural Science and Technology, Kanazawa University, Kanazawa 920-1192, Ishikawa, Japan
[2] Institute of Science and Engineering, Kanazawa University, Kanazawa 920-1192, Ishikawa, Japan
* Correspondence: jan@ums.ac.id or jan@stu.kanazawa-u.ac.jp

Abstract: Vehicle to everything (V2X) technology allows the broader development of driving safety, efficiency, and comfort. Because the vehicles can quickly send and receive frequent messages from other vehicles and nearby devices, e.g., cooperative awareness message applications on the intelligent transport system (ITS), V2X requires a good security and privacy protection system to make the messages reliable for the ITS requirements. The existing standards developed in the US and Europe use many short valid period pseudonym certificates to meet the security and privacy requirements. However, this method has difficulty ensuring that revoked pseudonym certificates are treated as revoked by any vehicles because distributing revocation information on a wireless vehicular network with intermittent and rapidly changing topology is demanding. A promising approach to solving this problem is the periodic activation of released pseudonym certificates. Initially, it releases all required pseudonym certificates for a certain period to the vehicle, and pseudonym certificates can be used only after receiving an activation code. Such activation-code-based schemes have a common problem in the inefficient use of network resources between the road-side unit (RSU) and vehicles. This paper proposes an efficient and privacy-preserving activation code distribution strategy solving the problem. By adopting the unicast distribution model of modified activation code for pseudonym certificate (ACPC), our scheme can obtain benefits of efficient activation code distribution. The proposed scheme provides small communication resource usage in the V2X network with various channel options for delivering activation codes in a privacy preserved manner.

Keywords: intelligent transportation systems; C-ITS; V2X; VANET; security; privacy; certificate revocation

Citation: Wantoro, J; Mambo, M. Efficient and Privacy-Preserving Certificate Activation for V2X Pseudonym Certificate Revocation. *J. Sens. Actuator Netw.* **2022**, *11*, 51. https://doi.org/10.3390/jsan11030051

Academic Editors: Michel Kulhandjian and Hovannes Kulhandjian

Received: 2 August 2022
Accepted: 27 August 2022
Published: 1 September 2022

1. Introduction

The automotive industry constantly tries to improve driving safety and efficiency by applying various cutting-edge technologies, one of which is V2X technology. The V2X enables vehicles to communicate with other vehicles, infrastructure, pedestrians, mobile networks, and any entity that the vehicle may affect or be affected by. The V2X communication goal is to enhance the safety and efficiency of transportation, and the killer applications are platooning, real-time congestion warning, emergency electronic brake lights, and so on.

There are some requirements for security and privacy in V2X [1]. First and foremost, security mechanisms ensure that sending and receiving messages can be authenticated and authorized by a reliable party. The V2X architecture must ensure message authenticity, which is usually achieved through digital certification to prevent abuse by drivers and the system itself [2]. The digital certificate can also ensure message permissions, but identity disclosure can violate driver privacy. Authentication frameworks need to provide privacy preservation mechanisms to prevent identity disclosure attacks, as unwilling identity disclosure and location tracking can violate the privacy of drivers and users.

A location tracking attack is an attempt to track the location and path of the vehicles during a specific period. For privacy preservation, V2X should not make a detailed lifelong

history of driver behavior available to others, which centers around the concept of unlinkability, so eavesdroppers cannot quickly identify or track owners of unrevoked vehicle certificates. Many groups of researchers have designed security solutions for V2X based on the public key infrastructure (PKI) [3]. For privacy protection purposes, they apply pseudonym certificates with a reasonably limited validity period which need to be changed regularly [2]. The pseudonym certificates are used to sign V2X messages such as the basic safety message that is periodically transmitted by vehicles or roadside units.

By providing multiple short-term pseudonym certificates to each vehicle, the certificate revocation mechanism becomes more complex in V2X PKI. Suppose the vehicle is provided with many certificates sufficient for long-term usage, e.g., for three years. In that case, revoking the certificate will overfill certificate revocation lists (CRL) very quickly [4]. To solve this problem, the United States (US) and European Unions (EU) take the following different approaches. The development of V2X PKI for cooperative intelligent transportation systems (C-ITS) in the EU decided to provide certificates only for thee months of use [5].

Consequently, the vehicle must periodically contact the certificate authority (CA) for new certificates. Generating a new pseudonym certificate requires a bidirectional connection. The periodic and bidirectional connection gives a significant addition to the overall cost of the system [6]. Conversely, the development of V2X PKI in the US, called the security credential management system (SCMS), decided to implement a linkage value and allow the vehicle to bring many certificates for three years of usage [2]. The linkage value allows all pseudonym certificates in one vehicle to be revoked using only one link seed record in the CRL. It is still a burden on the system, especially because the link seed of a revoked certificate will stay longer in the CRL even though the individual certificate is valid for only a short time.

Both standard approaches still need improvements in efficiency, especially in supplying pseudonym certificates and revoking misbehaved vehicles. A promising approach to reducing vehicle interaction with the CA while reducing costs caused by large CRL is to use the activation codes technique [7]. The idea is to encrypt the pseudonym certificate using a secret code before giving it to the certificate's owner. The certificate's owner must receive the code to activate (decrypt) their pseudonym certificate before being able to use it. Then, the activation codes are released periodically to all unrevoked vehicles, so each revoked vehicle in a new period cannot use its certificate because it does not receive the activation code for the recent period. Among the solutions that use this method is the ACPC [8]. The ACPC allows vehicles to obtain the activation code much more efficiently because it reduces the overall cost of certificate distribution and revocation by its unique caching property due to binary tree utilization of its activation code. By its caching property, ACPC can broadcast and place its activation code anywhere on a public site safely for rebroadcast or later retrieval. Using public devices without CA control, such as web servers, RSU, and cellular phones, reduces the V2X PKI infrastructure burden. It contrasts with periodic pseudonymous certificate issuance as described in European Telecommunications Standards Institute (ETSI) [9], which requires the vehicle to establish and maintain a secure connection to the CA for certificate renewal.

With the broadcast and caching capabilities of ACPC, the possible scenario is that the certificate access manager (CAM) broadcasts the activation code to RSU. The activation code in RSU makes it easier for vehicles to reach the activation code immediately because RSU is a device closest to the vehicle on the road. The RSU will easily receive activation code broadcasts from CAM because, topologically, it is a fixed device and is always active when the activation code broadcast is happening. In contrast, vehicles are mobile devices with intermittent wireless networks. Moreover, the vehicle is inactive when it stays in the garage or parking lot. This situation means the vehicles cannot receive the activation code broadcast, so the vehicle is more likely to request its activation code from RSU while it is active on the road.

In the original ACPC, the vehicle asks for an activation code via RSU as a cache device. The vehicle must receive all the broadcasted intermediate nodes of the binary tree, even though it only needs one of the obtained nodes to derive its activation code. The reason why such a construction is adopted is that the vehicle avoids showing its vehicle identity (`VID`) for privacy reasons. The `VID` is a vehicle identity that represents the binary tree leaf position, which is the location of the vehicle's activation code [8]. Eavesdroppers who happen to know `VID` can track the vehicle because each vehicle has a unique `VID`.

The ACPC allows vehicles to perform activation much more efficiently than the issue first activate later (IFAL) scheme because it utilizes the binary hash trees for efficient activation code broadcast as performed by the binary hash tree based certificate access management (BCAM) scheme [6]. The efficiency of the ACPC can be improved in the fixed-size subset (FSS), variable-size subset (VSS), and direct request (DR) by utilizing cache devices and picking several nodes for privacy preservation [10]. The DR is the most efficient scheme but cannot preserve privacy requirements. So, the activation code for pseudonym certificate (uACPC) [11] proposes not to use a fixed `VID` that matches the vehicle's long-term identifier. Unfortunately, uACPC violates the concept of privacy by design in SCMS (II.A. Threat Models and Application Concepts [2]), which imposes a condition that at least two SCMS components need to collude to gain meaningful information for tracking a vehicle. The registration authority (RA) alone is enough to have knowledge regarding the relationship between `VID` and long-term identity of the vehicle.

In this paper, we propose a scheme that optimizes the use of cache devices such as the RSU based on the ACPC design to achieve efficiency of activation code distribution on V2X communications while providing privacy preservation. Contributions of the paper are as follows:

- Our design ensures that during the certificate registration and activation code distribution only the vehicle knows its identity (`CID`) of the activation code to maintain the concept of privacy by design in SCMS.
- Our scheme provides a different `CID` for each activation period to avoid vehicle tracking during the unicast distribution model.
- Our scheme can benefit from the unicast distribution model for efficient activation code distribution.

The rest of this paper is organized as follows. Section 2 describes related work that has been completed so far to reduce the size and improve distribution efficiency of the activation code. Section 3 explains how we design our proposed scheme to meet our goal. Then we show and discuss the result of our schemes as well as the comparison in Section 4 and conclude our work in Section 5. For convenience of the reader, we define the symbols and notations used in Table 1. Since we built it on top of ACPC, most notations borrow from ACPC with some additions.

Table 1. General notation and symbols.

Symbol	Meaning
`node`	A binary tree node
I	Suffix security string
`cam_id`	Certificate access management identity
G	Elliptic curve group generator
E, e	Public and private caterpillar encryption keys
$\tilde{E}, \tilde{e}$	Public and private cocoon encryption keys, dedicated to the `CID` encryption and decryption
$\hat{E}, \hat{e}$	Public and private cocoon encryption keys, dedicated to the `pkg` encryption and decryption
$\hat{S}, \hat{e}$	Public and private cocoon signature keys that paired with $\hat{E}$ and $\hat{e}$

Table 1. *Cont.*

Symbol	Meaning
f_2, f_3	Pseudo-random function
f_4	Random choice function
β	Number of cocoon keys in pseudonym certificates batch
t	Pseudonym certificate time period
τ	Number of time period in pseudonym certificates batch
α	Number of activation time period
σ	Number of valid certificates each period
`cert`	A pseudonym certificate
`pkg`	An encrypted pseudonym certificate
`CID`	Code identity or binary tree leaf node position
$\mathbb{CID}$	Encrypted code identity
`code`	The value of leaf node or the activation code
A	blinded activation code
$Enc(str, \kappa)$	Encryption of bit-string str with key κ
$Dec(str, \kappa)$	Decryption of bit-string str with key κ
n_t	Number of total vehicle or number of total binary tree leaf
n_r	Number of revoked vehicle or number of marked (as revoked) binary tree leaf
n_b	Number of the binary tree node that distributed
$\|str\|$	Length of bit-string str, in bit

2. Related Work

2.1. Current Standard Approach

The standards and interoperability are critical in V2X. There is a directive mandating interoperable V2X between member states [12]. Notably, in the US and EU, there is convergence across all standards upon the elliptic curve digital signature algorithm (ECDSA) signature scheme [13]. To assure the privacy and the security of communications between stations, the presence of a trusted third party as a certificate authority is required. Hence, to maintain trust between stations, on the one hand, and trust between stations and authorities on the other hand, they build PKI for V2X. The V2X PKI is different from PKI in general because it must support a vast number of devices and must maintain a balance between security, privacy, and efficiency aspects [14]. Privacy in V2X PKI will be managed by issuing each vehicle a long-term authorization certificate and an additional number of short-term pseudonymous certificates. RSU and vehicles use pseudonym certificates to sign V2X messages. However, broadcast applications such as cooperative awareness basic service, decentralized environmental notification basic service, or infrastructure messages service require authentication, authorization, and integrity but not confidentiality.

The V2X PKI design by the ETSI and the United States Department of Transportation (USDOT) uses several CA and CRL to manage the credentials of vehicles [2]. The CRL method effectively blocks the revoked credentials that will check during each signature validation. However, it has several issues when applying the CRL method to the V2X PKI, especially when revoking the pseudonym certificate because the single revoked vehicle will involve many pseudonym certificate revocations. It will lead the CRL entry size to grow too large, which also affects the process of message verification [15].

With the anticipated scale of the massive vehicle network, the size of the CRL entries is likely to overgrow, especially since each vehicle carries from 20 to 100 pseudonym certificates per week. Large CRL entries are particularly problematic regarding the latency between receiving a signed message and verifying that the appropriate certificate is not on the revocation list. Message verification to the CRL should not take too long, especially for periodic service messages such as cooperative awareness messages, because it is a kind of real-time message type that is delay sensitive. As with the PKI architecture in general, how to effectively update the CRLs entries is also a problem in V2X PKI and is even more complicated. A CRL entry update to all vehicles is not easy because of the

limited connectivity of vehicular networks. Moreover, delayed CRL entry updates lead to vulnerability windows on the system, and a revoked pseudonym certificate is undetected during message certificates verification.

There are two different approaches that the US and EU standards use to deal with pseudonym certificate revocation problems. The ETSI ITS standard [5] provides only a limited number of pseudonym certificates for a short period (2–3 months). Consequently. the vehicle periodically connects to RA and receives its following pseudonym certificate more often. The RA will reject pseudonym certificate requests from revoked vehicles. However, revoked pseudonym certificates are still usable until they expire. So, it needs the CRL during this period, but because every single vehicle carries 20 to 100 pseudonym certificates per week, the number of CRL will be significantly large. However, the revocation criteria and the CRL distribution parameters on the Institute of Electrical and Electronics Engineers (IEEE) and ETSI are not yet defined [16].

On the other hand, the National Highway Traffic Safety Administration (NHTSA) in the US proposes a secure and modular architecture based on PKI where no components know the full set of certificates of a single device to avoid insider attacks on end-user privacy. It has defined the SCMS pilot project [17] with linkage-based revocation to reduce the CRL size. They use long-term and short-term enrollment certificates and the butterfly technology, where a single key (seed) is used to link every short-term certificate belonging to the vehicle. Only one key per vehicle revokes all its pseudonym certificates. However, the lifetime of the CRL entry corresponds to the total duration of the pseudonym certificate pool carried by the vehicle. With some short-term pseudonym certificates for three years of use, the identity of the revoked certificate remains in the CRL list for a long time (for example, three years). It is constantly checked with each vehicle verifying the message it receives. As a result, bandwidth usage for CRL distribution becomes a burden if many vehicles are unplugged. In addition, the vehicle processing fee to verify the certificate revocation status is relatively high. With approximately 300 million cars registered in the EU and US [18], vehicle resources are limited, and the stringent signature processing constraints of using CRL are far from ideal.

If we look at the different approaches of the two developed standards on how they manage revoked pseudonym certificates, it is clear that the pseudonym certificate revocation in V2X PKI still has fundamental problems that still need to be addressed so that V2X PKI can achieve its goal of maintaining security and privacy effectively.

2.2. Recent Research in Revocation Problems

Several recent papers have attempted to address the issue of certificate revocation by using blockchain technology. The Blockchain-Assisted Coded Caching Certificate Revocation List (BAC-CRL) [19] utilizes blockchain technology to help cache the CRL. TAs and RSUs in different regions are grouped into a blockchain network to manage and store their CRLs uniformly. Didouh et al. [20] perform blockchain integration for vehicle network cybersecurity by dynamically creating communities to uproot dangerous vehicles in real-time. The system is based on smart contracts and consensus, allowing vehicles to detect and remove dangerous vehicles in real-time. Perera et al. [21] propose certificate management based on blockchain structure and implement voting-based revocation to stop misbehaving vehicles from acting. They present a distributed framework for certificate management of a blockchain structure with a ring-signature-based voting process to provide secure and efficient certificate revocation. With the need for blockchain synchronization between V2X entities and additional blockchain mining processes, these schemes adopt a different architecture from the current standard. Security and privacy evaluation methods of current standards may not be directly applied to them. So they still require further study on whether all the V2X security and privacy requirements are fulfilled.

Wang et al. [22] propose a certificateless lightweight aggregate signature scheme with a revocation mechanism suitable for 5G-enabled vehicle networks. They use a "cuckoo" filter to build a revocation mechanism to prevent malicious vehicles from attacking again.

Their scheme is not PKI-based but based on an aggregate signature scheme and designed on 5G networks only. Mistarehi et al. [23] propose another certificateless scheme providing a low-overhead message authentication and dissemination. Unlike many existing schemes, this scheme does not use certificates and a CRL to provide authentication mechanism. Again, these schemes do not compatible with the current standard architecture.

As described in Section 2.1, it is a challenging goal to construct communication trust between between vehicles while maintaining user privacy. We try to achieve the goal by solving the revocation problem while maintaining compatibility with existing standards. One promising scheme that has compatibility with the existing standard while reducing the CRL problem is the ACPC [8]. It was developed based on SCMS [17] architecture, so it is equal to the current V2X PKI standard except for the certificate revocation mechanism. ACPC utilizes the activation code mechanism to manage the pseudonym certificate revocation problem. The latest paper we found close to the activation code mechanism is the uACPC [11]. The activation code mechanism is further discussed in the next section.

2.3. Promising Approaches for The Certificate Revocation Problems

To avoid high CRL growth while maintaining the performance improvements associated with butterfly key derivation, ACPC [8] builds on the IFAL [7] activation code concept and uses the standard approach of SCMS with some modifications. The ACPC uses a binary hash tree to broadcast activation codes as the BCAM [6] scheme does. It allows the vehicle to obtain activation codes much more efficiently than the IFAL scheme. Nevertheless, unlike BCAM, CAM in ACPC does not receive any certificates from RA, so CAM does not know that a group of the pseudonym certificates came from the same vehicle. So, the collusion between CAM and pseudonym certificate authority (PCA) does not allow the entity to track the vehicle. In addition, compared to the C-ITS approach with frequent certificate provisioning, one of the benefits of ACPC is that the activation code for an unrevoked vehicle is public information. It can even be cached anywhere (for example, in vehicles, roadside units, web servers, or mobile phones) for later retrieval. This caching property reduces the infrastructure load of V2X PKI.

However, ACPC has some problems with the distribution of the activation code through the broadcast model because the bandwidth usage may be higher than what is normally obtained with the CRL distribution [10]. The ACPC activation code takes only 16 byte, compared to a 117 byte pseudonym certificate, and even one activation code is used against multiple pseudonym certificates, making it much more efficient. However, the broadcast model for distributing activation codes does not really take full advantage of the smaller size. The ACPC assumes the activation code broadcast is proportional to the number of revoked vehicles in the system with binary hash tree adoption. Although such activation codes size growth is attached to the binary hash tree whenever a revocation is required, one important characteristic of ACPC is that vehicles do not need the entire broadcast code to decrypt their certificates. Each vehicle requires only one tree node value, which is in the path between the corresponding leaf and the root. Following the strategy of requesting only part of the activation tree on ACPC, the actual bandwidth cost of the vehicle could be significantly less than that obtained with the CRL or the frequent provision of pseudonym certificates.

Reducing bandwidth costs between infrastructure and vehicles on ACPC schemes is performed by allowing vehicles to request only a single node from all available activation trees on the cache device or the responder (activation code provider). However, this method cannot be completed because the use of `VID` as a code request parameter can threaten the privacy of the vehicle. By requesting a node of code that matches its `VID`, the vehicle needs to send its `VID` to the responder. This allows the dishonest responder to know the `VID` of each vehicle. Moreover, if the request is made on a public channel, the adversary can monitor which paths are used by the same `VID`, meaning that the path of the vehicle is also being tracked.

The ACPC uses the leaf position of a binary tree as a VID, where each leaf contains a code to activate the pseudonym certificate of the vehicle. In other words, one vehicle will have a single specific VID to identify the position of its activation code on the binary trees. Since every single vehicle has its own VID, requesting only one code by the vehicle will cause privacy issues.

2.4. Unicast Distribution of Activation Code and Its Privacy Issue

Simplicio et al. [10] and Cunha et al. [11] show how ACPC (and similar solutions based on activation trees, such as BCAM) can benefit from the unicast distribution model and propose modified ACPC, FSS and VSS, and uACPC, respectively. Unicast is the communication where a piece of information is sent from one sender to one receiver. Vehicles can reduce bandwidth usage when bidirectional connectivity is available to request the activation code. A vehicle can request its activation code directly from the system authority, just like the certificate request in ITS, but with much less bandwidth. The unicast distribution model requires the vehicle to reveal its identity, so the system authority can determine which activation code it should provide. Generally, disclosure of identity to the system authorities is not a problem. Moreover, using a location obscurer proxy (LOP) is a general requirement to eliminate sensitive information that can damage privacy during communication with a system authority. However, if the activation code request is addressed to a cache unit that is not managed by the system authority, disclosing the identity of such a vehicle is very risky, particularly if the communication is completed directly without any proxies or through insecure channels.

To balance the privacy and efficiency of the unicast distribution method applied to ACPC, selecting additional nodes from the deepest depths of the activation tree is required in the activation code request [10]. Thus, the vehicle must request more than one node on the path to its leaf or the leaf itself. The number of vehicles that can make the same selection of the selected nodes is calculated as crowd size. The crowd size indicates a level of privacy. The level of privacy depends on the number of nodes requested. So a higher number of picked nodes results in better privacy. There are two ways to determine the number of additional nodes that a vehicle must take, namely the FSS and VSS algorithms. The FSS determines the number of retrieved nodes based on the number of tree depths (D), i.e., if D is 40, then the number of taken nodes is also 40. Privacy on FSS is quite good when the number of revocations is small. Still, the crowd size value continues to decrease logarithmically with the revocation number increase. The VSS algorithm is introduced to give the vehicle a choice to the desired level of privacy. The VSS will increase the number of requested nodes to increase the expected crowd size. However, to achieve a 100% privacy level, VSS would be equivalent to taking all available nodes, resulting in no bandwidth efficiency.

The bandwidth usage of such a strategy grows much more slowly than CRL for SCMS and C-ITS, even if thousands of vehicles are revoked. However, having additional nodes for good privacy means additional bandwidth is also required. Meanwhile, the DR method is the most efficient bandwidth usage. With DR, the vehicle only needs one node on the path to its leaf or the leaf itself, so its use improves the bandwidth usage (one node = 128 bits). However, this design fails to provide privacy. The requester reveals its identity to the respondent or even eavesdroppers. To deal with this, the uACPC [11] proposes not to use a fixed vehicle identity (VID) that matches the vehicle's long-term identifier. The uACPC requires the RA to generate a different VID for each activation period so that the vehicle will use a different identity to ask for an activation code for each period. When receiving a request for pseudonym certificates from a vehicle, RA specifies a different VID for each activation period using the pseudo-random permutation function. Then the RA requests a blinded activation code to CAM by sending the desired VID. After receiving all blinded activation codes, the RA sends it to the vehicle together with the corresponding VID and also pseudonym certificates response from the PCA. However, uACPC violates the concept of privacy by design in SCMS, which imposes a condition that at least two SCMS components

need to collude to gain meaningful information for tracking a vehicle. The RA alone is enough to have knowledge regarding the relationship between VID and the long-term identity of the vehicle.

2.5. The ACPC Binary Hash Tree Activation Code

Our scheme uses the same activation code generation as the original ACPC. Here is how the activation code is generated for each activation period. The binary hash tree activation code is the core of the ACPC to achieve its efficiency. The ACPC activation code has the same security level with a smaller bit-string size (128 bits) than its predecessor BCAM (256 bits) [8]. The binary tree construction and the small size of the activation code can benefit the distribution process.

The CAM is in charge of managing activation codes from generation to distribution. Depending on how many activation periods t are needed, the CAM must specify all the activation codes at the beginning. This activation code is constructed in the form of a binary tree, as shown in Figure 1.

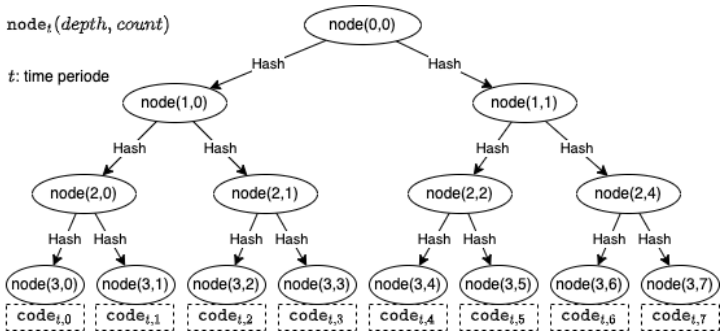

Figure 1. Binary tree activation code generation.

To maintain unlinkability, each activation code tree that is created must be completely different so that there is no relationship between the activation codes for each period. It starts by randomly assigning a value for the tree root $\texttt{node}_t(0,0)$ for each period t up to the desired τ time range. The desired security level is determined by the bit-string length k as in Equation (1). Then the CAM determines all the values of the $\texttt{node}_t$ in the binary hash tree construction (Equation (2)), each node is computed from its upper level node concatenated by a unique suffix security string I (Equation (3)), which is 104 bit length. It is designed to support 40-bit long CID for 2^{16} time periods, which means more than 1200 years if the time periods are 1 week.

$$\texttt{node}_t(0,0) = \{0,1\}^k \tag{1}$$

$$\texttt{node}_t(depth, count) = Hash(\texttt{node}_t(depth-1, \lfloor count/2 \rfloor) \| I) \tag{2}$$

$$I = (\texttt{cam\_id} \| t \| dept \| count) \tag{3}$$

The value in all leaf nodes is a code used to generate the encryption key during pseudonym certificate generation, so the vehicle cannot use its pseudonym certificate before obtaining that code.

3. Proposed Scheme

To provide better privacy preservation, we consider not using the leaf node position as a vehicle identity VID as in the ACPC described in Section 2.3. In our proposed scheme, one vehicle uses different identities for each activation period. In other words, the leaf node position is specific to the code identity, not the vehicle identity. Then, we use CID to denote the code identity to distinguish it from VID of the previous schemes. Unlike uACPC, which assigns the role of determining VID to RA, our scheme gives the right to generate CID to the CAM. It is essential to maintain the concept of privacy by design of the SCMS [2] to be

strong against attacks by insiders. The uACPC allows the RA to have information regarding the relationship between VIDs and the long-term identity of the vehicles. Meanwhile, our scheme does not allow the RA to learn the CID given to the vehicle by encrypting it before giving the encrypted CID to the vehicle through RA.

The CID to each activation code is different and randomly chosen, so it is hard for involved entities or the adversaries to conclude the relationship between CID and the vehicle identity because it has no direct relationship with them. It becomes hard to track vehicles through their CID, even though the vehicle exposes its CID to the responder to retrieve its activation code. Moreover, our privacy preservation scheme retains the positive property of ACPC such that codes can be placed safely on the public responder, and vehicles have more flexibility to retrieve their code from any public cached devices.

Here are our strategies to obscure the relation between binary tree nodes and the vehicle identities: First, we do not label the node position as a single vehicle identity or VID on the binary tree; otherwise we label the node position as a node identity or CID. Second, only the corresponding vehicle has the information about its CID. Third, the CID for every activation period is different and randomly chosen.

We do not label the node position as a single vehicle identity to emphasize the concept that the leaf node in the binary tree does not represent a particular vehicle entity. We change the term vehicle identity to code identity because it is the identity of the code, not the identity of the vehicle. So CAM can determine any leaf node to assign to any vehicle. That way, there is no special relationship between the identity of the code and the identity of the vehicle.

When CAM determines a leaf node to obtain a code for a vehicle, it randomly selects a node that has not been used by the previous vehicle. Even CAM has no knowledge of which vehicle is requesting the code in order to maintain the privacy of the vehicle. After determining the leaf node, the CAM converts the code into a blinded activation code and encrypts the identity code with the requesting vehicle's encryption key so that when handed back to RA, RA also does not obtain any information about the CID given by CAM to the vehicle. Only the vehicle itself can unlock the CID it receives using its pair of encryption codes. It means that only the corresponding vehicle has the information about its CID.

Our system architecture can be described in two parts. The first part shows the process of pseudonym certificates issuing to the vehicles by determining the CID and the encryption key for each certificate package generated by the collaboration of RA, CAM, and PCA. The second part presents activation code distribution scenarios that are supported by our proposed scheme, as well as the benefits derived from it.

3.1. Pseudonym Certificate Issuing

Before starting to issue a pseudonym certificate, the CAM needs to set an activation code for all the desired activation periods. This activation code is constructed in the form of a binary tree according to the construction in ACPC as described in Section 2.5. We choose this construction because it has a small activation code that can benefit the distribution process. After all the activation code construction in the binary tree form is complete, vehicles can start registering to obtain their respective pseudonym certificates. The pseudonym certificate issuing phase can be described as shown in Figure 2. Then, for the details of the process for each entity involved, it can be seen in Figure 3.

The vehicle starts by supplying a randomly selected *caterpillar* private key s and e with the corresponding public *caterpillar* key $S = s \cdot G$ and $E = e \cdot G$. The keys s and e are for signing and encryption, respectively. They also pick up two random seeds to initialize the pseudo-random functions f_1 and f_2 for later butterfly key expansion constructs, as was performed in the SCMS design. Then the vehicle includes $(S, E, f1, f2)$ as a certificate

request message to RA to trigger the creation of the number of β certificates divided into several τ activation periods, where σ is the number of certificates per period.

$$\beta = \tau \cdot \sigma \tag{4}$$

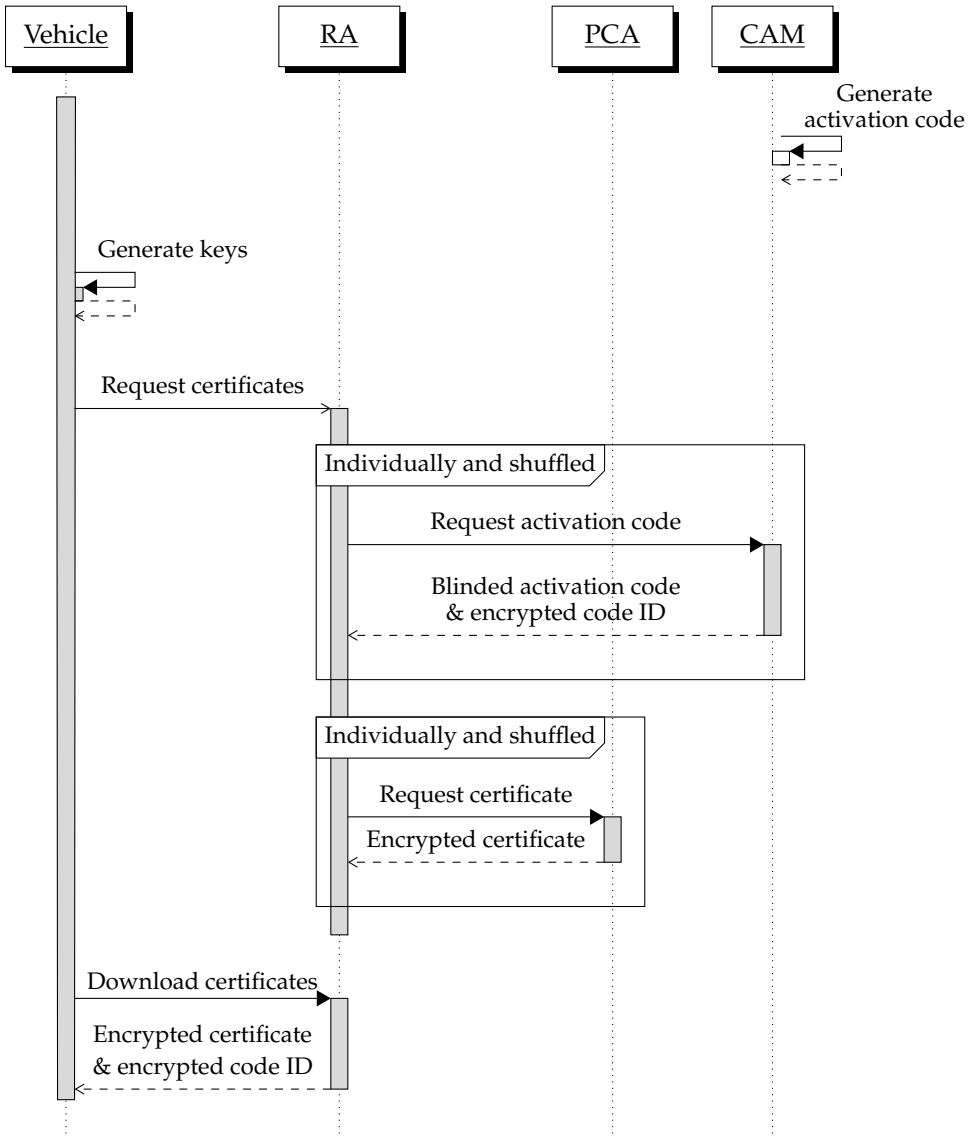

Figure 2. Pseudonym certificate issuing phase.

Since the S and $f1$ parts are unchanged in our construction and remain consistent with the original SCMS design, their process details are not included in the diagram shown in Figure 3 to simplify the explanation. However, the RA must send the public *cocoon* key $\hat{S}_t$ and $\hat{E}_t$ pairs together to the PCA.

Before RA generates a public cocoon encryption key $\hat{E}$ to encrypt the certificate, it first creates a public cocoon encryption key $\tilde{E}_t$ (Equation (5)) and sends it to the CAM for blinded activation code A_t request. In order not to violate privacy goals, the system needs to prevent the CAM from knowing if two $\tilde{E}_t$ belong to the same vehicle. The RA must have a configuration parameter for shuffling, i.e., shuffling 10,000 requests from different vehicles or waiting for all requests in one day. This shuffle mechanism is also applied to RA and PCA communications for the same reasons described in [24].

$$\tilde{E}_{t_c} = E + f_2(t) \cdot G \tag{5}$$

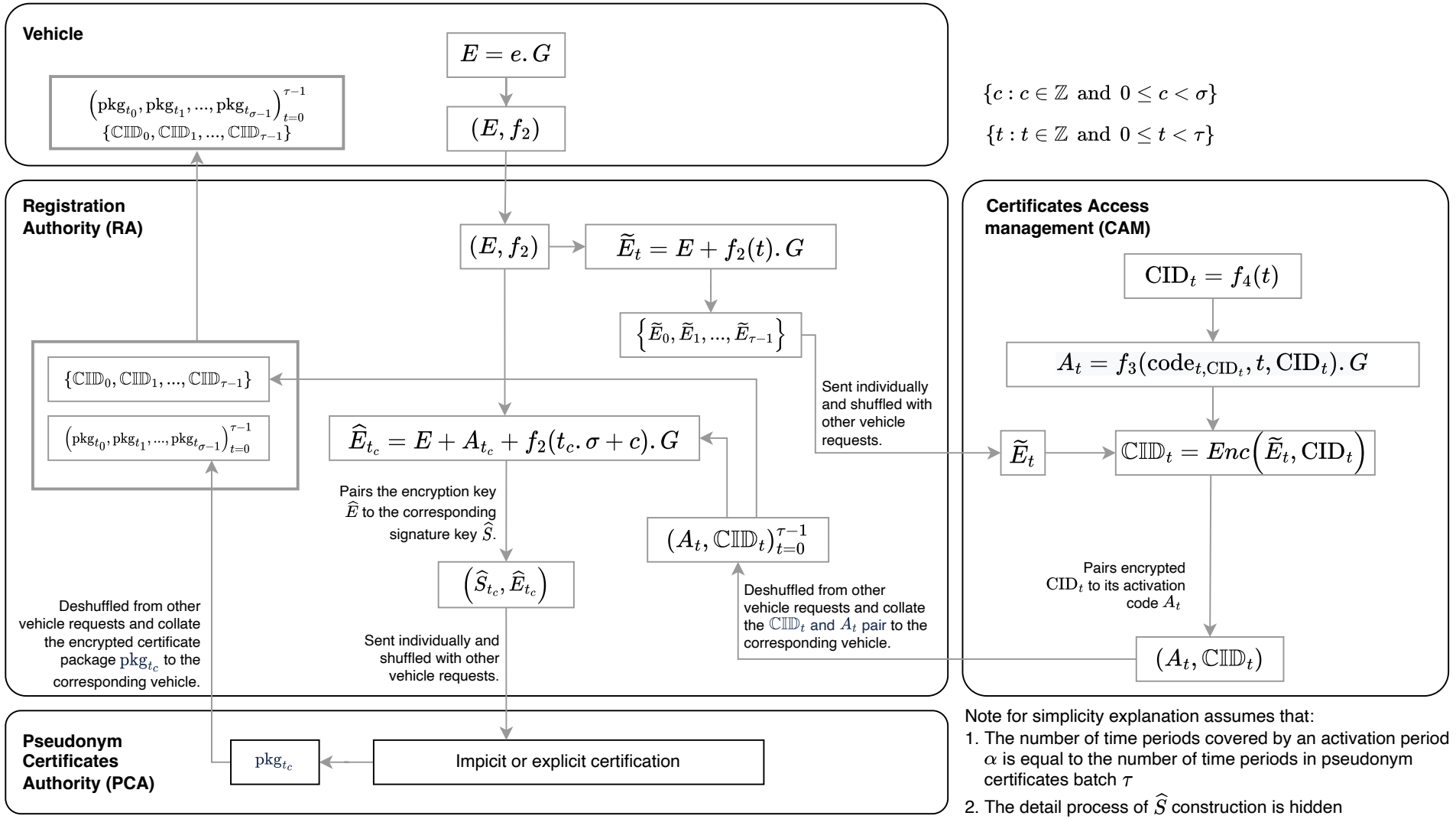

Figure 3. Pseudonym certificates issuing diagram.

During the activation code request, CAM will randomly select an available CID (not already used by other vehicles) every time period t using the random selection function f_4. Based on the selected $\texttt{CID}_t$, CAM obtains $\texttt{code}_t$ from the binary tree leaf $\texttt{node}(depth, count)$. The *depth* parameter is the bit-string length $|\texttt{CID}|$, and the *count* is the CID itself. Note that each CID can be associated with a single tree leaf because the tree depth matches the bit-length of CID. The pseudo-random function f_3 then generates a blind activation code A_t. The selected $\texttt{CID}_t$ that applies to the f_3 function is then encrypted by $\tilde{E}_t$ and pairs the result $\mathbb{CID}_t$ with the blind activation code A_t.

$$\texttt{CID}_t = f_4(t) \tag{6}$$

$$\texttt{code}_t = \texttt{node}_t(|\texttt{CID}|, \texttt{CID}) \tag{7}$$

$$A_t = f_3(\texttt{code}_t, \texttt{CID}_t, t, \texttt{CID}_t) \cdot G \tag{8}$$

$$\mathbb{CID}_t = Enc(\texttt{CID}, \tilde{E}_t) \tag{9}$$

The CAM completes every single request from the RA with one cycle of generating a blinded activation code and encrypting the associated $\texttt{CID}_t$. Paired $\mathbb{CID}_t$ and A_t are then returned to RA, deshuffled, and collected according to the requesting vehicle. The A_t is used as an additional parameter for the encryption key $\hat{E}_t$ generation together with the expansion function f_2, as shown in Equation (10). Then, $\hat{E}_t$ is used in pairs with the public *cocoon* keys $\hat{S}_t$ to generate a pseudonym certificate by PCA as performed in SCMS [2]. The pseudonym certificate package $\texttt{pkg}_{c,t}$ generated by the PCA sends to RA, then RA gives it to the vehicle together with related $\texttt{CID}_t$, where $0 < t \leq \tau$ and $0 < c \leq \sigma$.

$$\hat{E}_{t_c} = E + A_{t_c} + f_2(t_c \cdot \sigma + c) \cdot G \tag{10}$$

In this way, even though the CAM determines the $\texttt{CID}_t$ along with the appropriate A_t for each request, it does not know which vehicle is requesting it. By the encrypted $\mathbb{CID}_t$ and blinded A_t made by CAM, the RA also does not have information about $\texttt{CID}_t$ and $\texttt{code}_t$ given to the vehicle. Furthermore, PCA does not have any information about it either. It can be said that only the requesting vehicle knows the $\texttt{CID}_t$ after decrypting the $\mathbb{CID}_t$ as a reference to obtain the appropriate code for its certificates.

3.2. Activation Code Usage

The stages of distribution and the activation code usage by vehicles can be seen in Figure 4. In order for the vehicle to request its activation code, the vehicle needs to know the $\texttt{CID}_t$ for the next activation period. The vehicle computes the $\tilde{e}$ as a key to decrypt $\mathbb{CID}_t$, as shown in Equations (11) and (12). On the other side, the CAM must distribute the activation codes before the validity period of the current pseudonym certificates expires. The CAM distributes the activation code through the responder units. Then the vehicle uses the given $\texttt{CID}_t$ as a parameter when requesting a specific activation code from the responder.

$$\tilde{e}_t = e + f_2(t) \tag{11}$$

$$\texttt{CID}_t = Dec(\mathbb{CID}_t, \tilde{e}_t) \tag{12}$$

The responder will look for the requested code in its chacing unit according to the received CID. Once it is found, the activation code is immediately send back to the vehicle. However, if there is no activation code that matches the CID, the CAM will give an invalid response to the vehicle. After the vehicle receives its activation code, the vehicle uses it to compute the $\tilde{e}_t$ value (Equation (13)). Then, the vehicle decrypts its pseudonym certificate using the $\hat{e}_t$. The complete diagram for the certificate activation can be seen in Figure 5.

With active pseudonym certificates, vehicles can use them for message authentication on required V2X applications.

$$\hat{e}_t = e + f_3(\texttt{code}_{t,\texttt{CID}_t}) + f_2(t_c \cdot \sigma + c) \tag{13}$$

$$\texttt{cert}_{t_c} = Dec(\texttt{pkg}_t, \hat{e}_t) \tag{14}$$

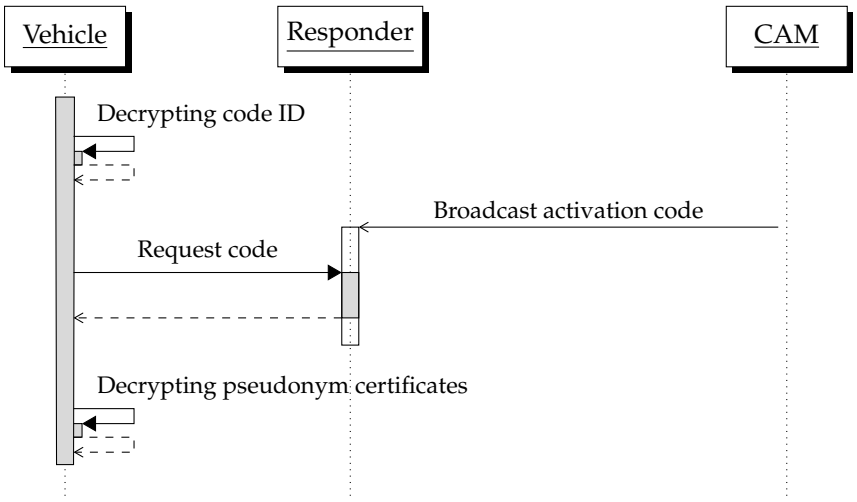

Figure 4. Activation code issuing and usage phase.

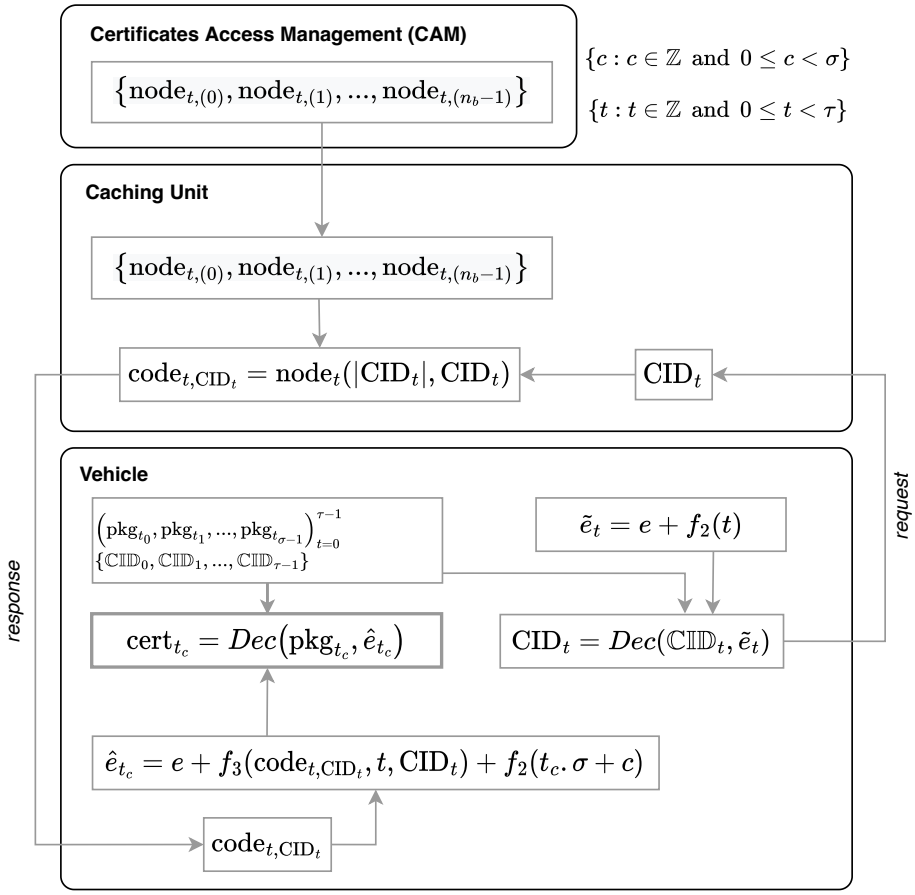

Figure 5. Certificate activation diagram.

3.3. Activation Code Distribution Scenarios

All vehicles require an activation code to use their certificate in each period. In our scheme, the activation code can be sent through various channels to make it easier for the vehicle to choose the best channel around it. For mobile networks, the delivery is performed in a unicast communication manner, i.e., the vehicle will ask the RSU, cellular tower, or public cloud to obtain its activation code, see Figure 6. Then the V2X network only uses 40 bits `CID` for upload and 16 bytes (128 bits) for downloads per vehicle activation period.

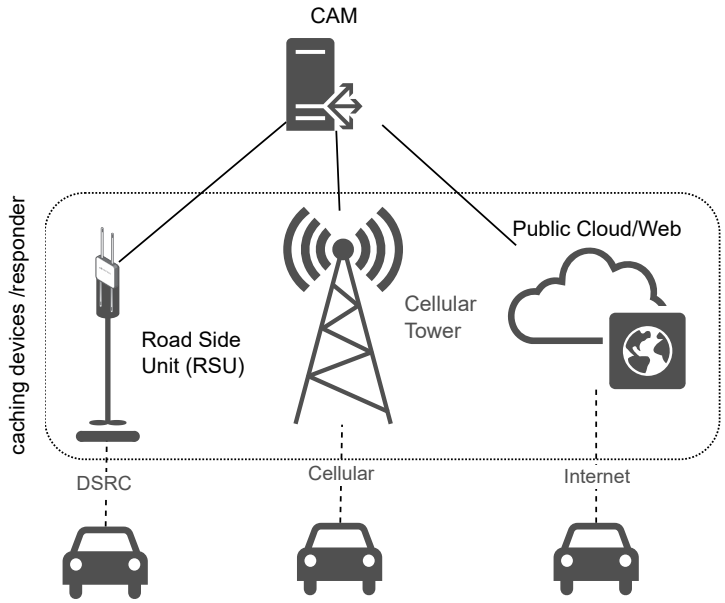

Figure 6. Caching strategy distribution.

There are four possible scenarios for sending an activation code to the vehicles.

1. Input manually

   The manual input method is not a practical way. However, it is easy for the users to manually enter the code in the vehicle on-board unit (OBU) devices after users receive the code through communication media such as email or short message service (SMS). It is also possible that users obtain code from a vehicle service such as a repair shop or gas station, then enter the code manually into the vehicle OBU devices. However, this method is only possible if the activation code period is not too short, say a month or more. If the activation period is only a few hours or minutes, this method is not very useful.
2. Broadcast periodically

   Subscribed devices can receive all codes from the CAM periodically. Vehicles that have a good Internet connection can receive codes in this mode. A direct send activation code from CAM to vehicles is not the best choice since it burdens the CAM server and takes no advantage of binary tree construction. Moreover, this setup is hampered in practice by the situation that the OBU in the vehicles is typically only active when the vehicle is. However, the responder device that will serve the activation code request from the vehicle also receives the activation code in this mode, for example, RSU, repair shop, gas station, or web server. All of these devices are pretty easy to obtain an activation code from periodically because they are always live and stationary devices with a stable network connection to the CAM.
3. Point-to-point communication

   It is a direct interaction between the CAM and the vehicle. If all vehicles have a strong Internet connection, point-to-point communication is accessible. Another method used is the short message service (SMS) proposed by [7]. However, such a connection requires users to have some subscription contracts with the service

provider at additional costs. Moreover, the Internet network cannot support the whole area, for example, the suburbs.
One possible way is through the road infrastructure network. The vehicle is wirelessly connected using dedicated short range communications (DSRC) technology via the RSU along the road. The RSU then forwards it to the Internet network so the vehicle can communicate with the CAM. However, it possibly overloads the CAM and RSU.

4. Indirect communication
   It means that the vehicle does not receive an activation code directly from the CAM but from the caching devices or responder, such as a proxy server on the Internet network or the RSU. The responder is a device that has previously received all the codes from the CAM broadcast periodically. Responders can be web servers, vehicles, or RSU. Vehicles can use one of the responders available in the surroundings by requesting an activation code based on the selected `CID`.

All of the above communication scenarios can be used simultaneously, thus providing many options for vehicles to obtain the activation code quickly. Even so, the first to third scenarios can generally also work on the original ACPC. Therefore, we are more interested in discussing the efficiency that occurs in indirect communication, especially when using RSU as the responder. If bidirectional connectivity is available for a binary-tree-based activation code, it can benefit from a unicast distribution model. Vehicles can greatly reduce bandwidth usage when requesting an activation code. The main purpose of the V2X network is to transmit information that relates to driving safety and efficiency, and this main purpose should not be interfered with by other applications. The efficient bandwidth usage by V2X PKI is very beneficial for the V2X network.

To obtain optimal benefits of binary tree construction, we utilize a cache unit that acts as a responder. Responders can respond to vehicle requests for activation codes, as shown in Figure 7. The closest unit to the vehicle on the road is the RSU. If the RSU becomes a responder activation code, it provides the activation code easy access by the vehicles.

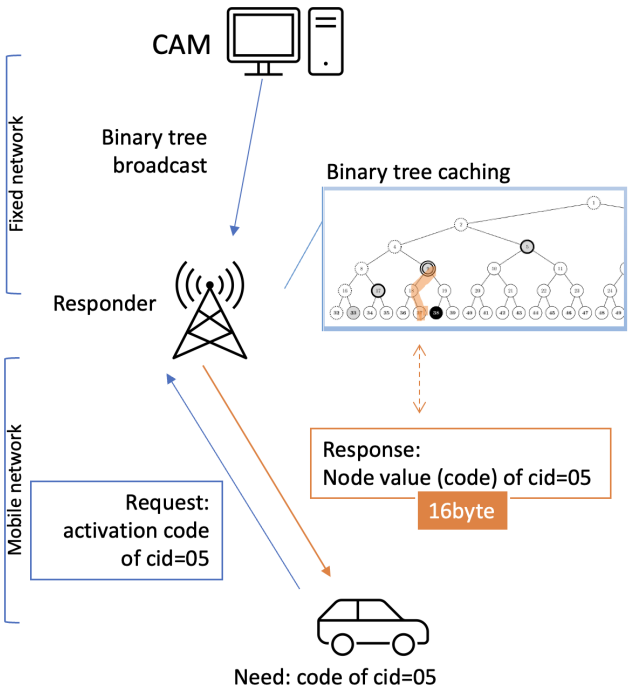

Figure 7. Unicast distribution.

With a different `CID` for each period as described in Section 3.1, even if the certificate authority does not control the responder, the vehicle can request an activation code to the responder without worrying about its privacy. The untrusted responder cannot track the

vehicle path based on the exposed CID. After the vehicle decrypts its CID, the vehicle can safely show its CID to ask the responder for the activation code.

Bandwidth usage on the mobile network for activation code transmission is achieved in a minimum size because the activation code sent from the responder to the vehicle is only one code (16 byte). Moreover, the cache unit utilization reduces the certificate authority burden and provides more alternatives for the vehicles to obtain their activation code.

4. Analysis of the Proposed Scheme

4.1. Unicast Distribution Model

All vehicles require an activation code to use their certificate at activation period t. For efficient activation code distribution to every vehicle on the V2X network, primarily via RSU, the activation code is sent through the broadcast and unicast distribution mechanism. In the broadcast mechanism, CAM sends the set of the activation code in period t. The broadcasted activation codes are received and stored by the RSU. Due to the reliable network between them, there are relatively no problems with the broadcast distribution to the RSU. However, it is likely impossible that all vehicles will receive the broadcasted file concurrently. Whether the vehicles are out of network or in an inactive state during parking is very likely to happen. Although it is possible to keep the OBU active while the vehicle is parked, the possibility for the vehicle to be inactive still occurs.

4.2. Privacy Protection: Different Code Identity in Each Activation Period

On the unicast distribution, the vehicles can request the activation code by showing their CID, so the RSU can immediately respond to the correct activation code. The ACPC has a privacy issue when using this unicast model, so it tries to solve this issue by increasing the crowd size privacy level [10]. However, it is still not working for DR because ACPC uses VID as vehicle identity to specify its activation code. Our scheme provides better privacy protection for the DR method, so it is possible to maintain minimum bandwidth usage in V2X for activation code transmission. Our scheme provides a different CID for each activation period to prevent vehicle tracking as also proposed in uACPC [11]. The different CID technique is inspired by V2X PKI, which uses different certificates to prevent vehicle tracking by others using vehicle communication paths.

During the unicast activation code distribution, the responder knows the CID of the vehicle for a single period only, and the activation code request will use a different CID in the next period, so the responder or eavesdropper has no idea whether it came from the one vehicle or not. Moreover, if the responder answers the activation code request at the first request attempt, the vehicle exposes its CID only once. So, this scheme provides the unlink-ability requirement of V2X privacy.

4.3. Privacy Protection: Hiding the Code Identity from V2X PKI Entity

The CID is used by the vehicle to request its corresponding activation code. None of the SCMS entities can fully know information about the CID given to a vehicle. The CID is encrypted using a key based on the vehicle's public key so that only the vehicle can find its CID by decrypting using its key pair. If the vehicle discloses its CID when requesting an activation code, no V2X PKI entity can associate the CID with another CID during activation so that the privacy of the vehicle can be maintained because each time it uses a different CID, it will be considered a different vehicle by the V2X PKI. This technique is the same as the pseudonym certificate used in the V2X PKI for privacy protection during periodic message sending.

Unlike uACPC, which assigns the role of determining VID to RA, our scheme gives the right to generate CID to the CAM. It is essential to maintain the concept of privacy by design of the SCMS [2] to be strong against attacks by insiders. The uACPC allows the RA to have information regarding the relationship between vids and long-term identity of the vehicles. Meanwhile, our scheme does not allow the RA to learn the CID given to the vehicle by encrypting it before giving the encrypted CID to the vehicle through RA.

4.4. Bandwidth Efficiency

The caching strategy applied to the activation code is to overcome the problem of connection and bandwidth limitations on the V2X network. By sending the entire activation code through a device connected to the reliable (non-mobile) network only, the activation code broadcast does not flood the V2X network. For comparison, let us say that $D = 40$ is the binary tree depth and the available leaf node to cover all active vehicles is $n_t = 2^D =$ 1,099,511,627,776 (about one trillion). If out of the total number n_t of vehicles there are $n_r = 50,000$ revoked vehicles, then the average number of nodes broadcast n_b by CAM is $n_r * log_2(n_t/n_r)$ for $1 \leq n_r \leq n_t/2$ [25]. The number of variable node v_n on VSS is dependent on vehicle request security level [10], while to reach maximum security level 100% on VSS, the v_n is equal to n_b. We assume that the first source of the activation code is CAM, although, in IFAL, it is the enrollment authority. However, in the context of broadcast activation code, they perform the same task.

From Table 2, it can be seen that ACPC and its descendants, including our scheme, can distribute the activation code more efficiently than the IFAL; the total activation code size of ACPC is 16 byte $* n_b = 1,420$ Mbyte. The enormous download size from CAM to RSU happens in the IFAL scheme because it has to send all activation codes to each unrevoked vehicle. The size of the IFAL activation code is 16 byte and 5 byte of the epoch identifier, with an additional 7 byte of the code identifier [7]. So, the IFAL activation code for all unrevoked vehicles in total is 27 byte $* (n_t - n_r) =$ 29,686,679 Mbyte.

Table 2. Performance cost under example parameters.

	IFAL	ACPC	uACPC	FSS	VSS	Our Scheme
CAM to RSU:						
Download (Mbyte)	29,686,679	1420	1420	1420	1420	1420
RSU to Vehicle:						
Upload (byte)	7	-	5	200	462,784	5
Download (byte)	27	1,419,720,267	16	640	1,480,908	16
Storage Usage:						
in RSU (Mbyte)	29,686,679	1420	1420	1420	1420	1420

Comparison setting:	
D	= 40
n_t	= 2^D = 1,099,511,627,776
n_r	= 50,000
n_b	= $n_r * log_2(n_t/n_r)$ = 88,732,517
$V_n(10\%)$	= 92,557
Notation:	
D	= binary tree depth
n_t	= total number of vehicles
n_r	= number of revoked vehicles
n_b	= number of broadcasted binary tree nodes
$V_n(10\%)$	= number of distributed binary tree nodes for 10% VSS privacy level

The storage required by the RSU to keep the activation code is equal to the activation code download size from CAM to RSU. The RSU must store $27(n_t - n_r) =$ 29,686,679 Mbyte activation code for IFAL. With such a large size for one activation period, it is difficult to expect IFAL to use a scenario with the RSU is an activation code responder. With this, we will remove IFAL from the communication scenario between the vehicle and the RSU. As for ACPC, uACPC, FSS, VSS, and our scheme, the storage space required in RSU is only $16n_b = 1420$ Mbyte. After RSU receives all the activation codes, the vehicle can request an activation code from it.

From upload and download size, the table shows that our scheme, uACPC, and IFAL use a small amount of data because they request only a specific node from which the vehicle activation code is derived. Changes in the number of revoked vehicles or active vehicles have no effect on upload and download sizes between RSU and vehicle. Meanwhile, there are no uploaded data for ACPC data, but the size of downloaded data by the vehicle is the same as the data transmitted from CAM to RSU, which is $16n_b = 1420$ Mbyte. Overall,

looking at all the total data transmitted from CAM to RSU and RSU to the vehicle, uACPC and our scheme use the smallest network resources.

4.5. Storage Usage

The storage usage on the vehicle is determined by the size of the certificate S_{pc} and how many certificates must cover the entire validity period τ. assuming that the pseudonym certificate file size S_{pc} is similar for all schemes with roughly 128 byte. To simplify the calculation let us say that one certificate is sufficient to cover one t, the total certificate size is $S_{pc} * \tau$. Total activation period α is the total period a that every a covers some certificates batch. Each certificate has a t validity period, and the entire validity period τ is the sum of t. Our scheme needs to store S_D byte of `CID` that is used for each a period, so our total storage usage is $(S_{pc} * \tau) + (S_D * \alpha)$. If we give setting $t = 5$ min and $a = t$, the storage requirement on the vehicle of our schemes and uACPC is slightly higher than IFAL, ACPC, FSS, and VSS. It is because the vehicle has to store all `CID` which is 40 bits per activation period.

As shown in Figure 8, if the certificate is prepared for three years of use as recommended by SCMS, then the vehicle will need approximately 40 Mbyte of storage space to store the pseudonym certificates and `CIDs`. Meanwhile, if the certificates are prepared for 10 years usage, the vehicle must have a minimum of 140 Mbyte storage space. By looking at the size of the stored data in the vehicles in varied years, our scheme is not significantly different than other systems. So there is no restriction in the storage usage of the vehicle OBU.

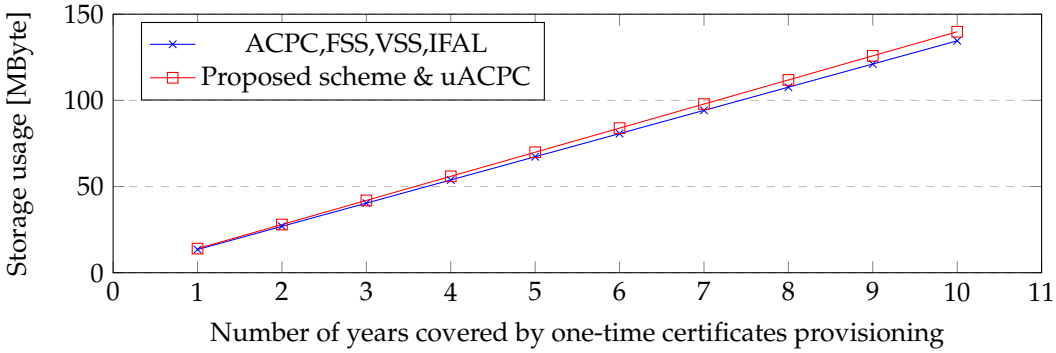

Figure 8. Storage usage in the vehicle.

4.6. Reducing Vulnerability Window

The number of nodes from ACPC that a vehicle must download varies depending on the number of revoked vehicles. Shortening the certificate validity and activation period together gives malicious vehicles less time to continue using the remaining certificates. Consequently, all vehicles have to download the tree node for their activation code more often. Considering the size of the activation code, which is relatively simple on the distribution, allows V2X PKI to minimize windows vulnerabilities. Our proposed scheme allows for a shorter certificate activation period with a small node size to be downloaded by a vehicle. In addition, the nodes distributed by CAM can be placed anywhere openly and securely. This property also allows decentralized distribution of activation codes to reduce the CAM load and give vehicles more options to obtain their activation codes as soon as possible.

Consider the vehicle's bandwidth usage to download the tree node over a certain period. If there are 50,000 revoked vehicles n_r out of a total of vehicles $n_t = 2^D$ with $D = 40$, then the size of nodes is S_a each t period The vehicle must download the $S_a * \alpha$ of total nodes size. Assume that we shorten the certificate validity t to 5 min only, and the total valid period is 1,576,800 min (3 years) total certificates as well as τ is 315,576. The i is the number of t that is covered by one a. With a variation of i, we can see by the graph in Figure 9 that our scheme compared to VSS and FSS uses the smallest total download of node size during three years usage. On average, as shown in Figure 9a, the average VSS is

required to download the most significant amount of data, and the most extensive data size is reached when the activation period is equal to one pseudonym certificate validity period with 29.19 GByte in total.

Although much lower than VSS, the FSS also has the same trend as VSS as shown in Figure 9b. Our proposed scheme shows that the total data downloaded for various cover validity periods for each activation period is minimal. The most interesting point here is that our proposed scheme is always below 1.48 Mbyte on average in all variations of the covered certificate validity period. Even if the activation period is equal to the validity period of a certificate, our scheme only needs to download 5 Mbyte of nodes in total to each vehicle during three years of usage. This result shows that our scheme is very good at network bandwidth usage between RSU and vehicles for a short activation period.

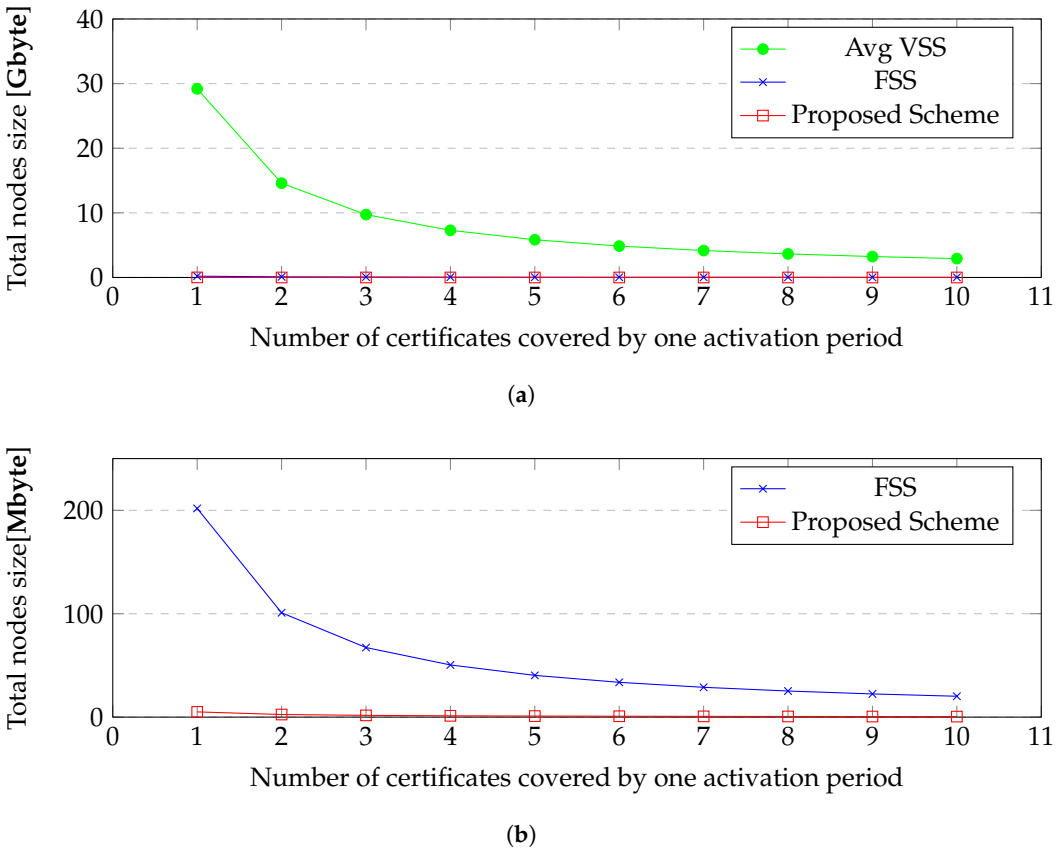

Figure 9. The total amount of downloaded nodes by a vehicle in 3 years. (**a**) Comparison among average VSS, FSS, and proposed scheme. (**b**) Comparison between FSS and proposed scheme.

4.7. Overall Comparison

In general, our scheme has the advantage of small file size in the distribution of the activation code in the unicast distribution model. However, our strategy needs a mechanism to ensure privacy preservation during the activation code distribution, one of which is encrypting the identity of the activation code. Consequently, there is an additional cost to decrypt the encrypted `CID` in the vehicle. The comparison in Table 3 shows that only our scheme has additional computational costs to decrypt the identity of the activation code. So it is necessary to consider the computational resources in OBU. However, the decryption of `CID` should not interfere with the daily operation of OBU because the decryption of `CID` can be performed when OBU is not busy with its routine tasks while on the road. For example, decryption is performed on all `CID` immediately after receipt, so there is no need to decrypt in the future. However, the computational cost can be acceptable with the efficient use of bandwidth, the ease of obtaining activation codes, and the privacy protection offered.

Table 3. Comparison of activation-code-based schemes.

	IFAL	ACPC	uACPC	FSS	VSS	Our Scheme
Distribution model:						
- Prevered	Unicast	Broadcast	Unicast	Unicast	Unicast	Unicast
Privacy protection:						
- Different code identity each activation period	No	No	Yes	No	No	Yes
- Hiding the code identity from V2X PKI entity	No	Yes	No	No	No	Yes
Bandwidth efficiency:						
- CAM to Responder bandwidth cost	Very High	Medium	Medium	Medium	Medium	Medium
- Responder to Vehicle bandwidth cost	Very Low	Medium	Very Low	Low	Medium/Low	Very Low
Storage usage:						
- In the responder	Very High	Medium	Medium	Medium	Medium	Medium
- In the vehicle	Medium	Medium	High	Medium	Medium	High
Computational cost:						
- Decrypting the activation code identity	No	No	No	No	No	Yes

5. Conclusions

In this paper, we have shown a scheme that increases the efficiency of communication between RSU and vehicles by improving activation codes distribution over the ACPC scheme. Our scheme fully utilizes the ability of ACPC, which can take advantage of caching devices openly without requiring control from a certificate authority.

We introduce an architecture to maintain the privacy of the activation code owner by providing a different code identity for each activation period. We also protect against possible insider attacks on the system by not allowing any entities to have information of the `CID` belonging to the vehicles.

The number of distributed activation codes is smaller than the previous scheme because the vehicle can request one specific code due to privacy protection of the `CID`. This small size of activation code then becomes advantageous for the V2X PKI system to reduce windows vulnerability against revoked vehicles.

The placement of the activation code in any caching device does not require encryption and authorization. The caching devices do not require any certificate authority control and do not burden the CAM. The activation code can be placed anywhere so that it is easily accessed by vehicles. This flexibility can increase vehicles' probability of reaching their activation code as soon as possible.

As future work, we will examine how to determine the optimal management and settings for our proposed scheme by via simulations.

Author Contributions: Conceptualization, J.W. and M.M.; methodology, J.W. and M.M.; software, J.W.; validation, J.W. and M.M.; formal analysis, J.W.; investigation, J.W. and M.M.; writing—original draft preparation, J.W.; writing—review and editing, J.W. and M.M.; visualization, J.W.; supervision, M.M.; project administration, J.W. and M.M.; All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The first author would like to thanks Ministry of Education, Culture, Sports, Science and Technology Japan (MEXT) and Japan International Cooperation Agency (JICA) for funding the scholarship to study at Kanazawa University.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

ACPC	Activation Code for Pseudonym Certificate
BCAM	Binary Hash Tree Based Certificate Access Management
C-ITS	Cooperative Intelligent Transportation Systems
CA	Certificate Authority
CAM	Certificate Access Manager
CRL	Certificate Revocation Lists
DR	Direct Request
DSRC	Dedicated Short Range Communications
ECDSA	Elliptic Curve Digital Signature Algorithm
ETSI	European Telecommunications Standards Institute
EU	European Union
FSS	Fixed-Size Subset
IEEE	Institute Of Electrical And Electronics Engineers
IFAL	Issue First Activate Later
ITS	Intelligent Transport System
LOP	Location Obscurer Proxy
NHTSA	National Highway Traffic Safety Administration
OBU	On-Board Unit
PCA	Pseudonym Certificate Authority
PKI	Public Key Infrastructure
RA	Registration Authority
RSU	Road-Side Unit
SCMS	Security Credential Management System
uACPC	Activation Code For Pseudonym Certificate
US	United States
USDOT	United States Department Of Transportation
V2X	Vehicle To Everything
VSS	Variable-Size Subset

References

1. Huang, J.; Fang, D.; Qian, Y.; Hu, R.Q. Recent Advances and Challenges in Security and Privacy for V2X Communications. *IEEE Open J. Veh. Technol.* **2020**, *1*, 244–266. [CrossRef]
2. Brecht, B.; Therriault, D.; Weimerskirch, A.; Whyte, W.; Kumar, V.; Hehn, T.; Goudy, R. A security credential management system for V2X communications. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 3850–3871. [CrossRef]
3. Hasan, M.; Mohan, S.; Shimizu, T.; Lu, H. Securing vehicle-to-everything (V2X) communication platforms. *IEEE Trans. Intell. Veh.* **2020**, *5*, 693–713. [CrossRef]
4. Raya, M.; Jungels, D.; Papadimitratos, P.; Aad, I.; Hubaux, J.P. *Certificate Revocation in Vehicular Networks*; Laboratory for computer Communications and Applications (LCA) School of Computer and Communication Sciences, EPFL: Lausanne, Switzerland, 2006; pp. 1–10.
5. ETSI. *Intelligent Transport Systems (ITS); Security; ITS Communications Security Architecture and Security Management*; Technical Report TS 102 940, V1.3.1; European Telecommunications Standards Institute: Sophia Antipolis Cedex, France, 2018.
6. Kumar, V.; Petit, J.; Whyte, W. Binary Hash Tree Based Certificate Access Management for Connected Vehicles. In Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Boston, MA, USA, 18–20 July 2017; Association for Computing Machinery: New York, NY, USA, 2017; pp. 145–155. [CrossRef]
7. Verheul, E.R. Activate Later Certificates for V2X–Combining ITS Efficiency with Privacy. Cryptology ePrint Archive, Report 2016/1158. 2016. Available online: https://eprint.iacr.org/2016/1158 (accessed on 1 August 2022).
8. Simplicio, M.A.; Cominetti, E.L.; Patil, H.K.; Ricardini, J.E.; Silva, M.V.M. ACPC: Efficient revocation of pseudonym certificates using activation codes. *Ad Hoc Netw.* **2019**, *90*, 101708. [CrossRef]
9. ETSI. *Intelligent Transport Systems (ITS); Security; Trust and Privacy Management; Release 2*; Technical Report TS 102 941—V2.1.1; European Telecommunications Standards Institute: Sophia Antipolis Cedex, France, 2021.
10. Simplicio, M.A.; Cominetti, E.L.; Patil, H.K.; Ricardini, J.E.; Silva, M.V.M. Revocation in Vehicular Public Key Infrastructures: Balancing privacy and efficiency. *Veh. Commun.* **2020**, *28*, 100309. [CrossRef]
11. Cunha, H.; Luther, T.; Ricardini, J.; Ogawa, H.; Simplicio, M.; Patil, H.K. uACPC: Client-Initiated Privacy-Preserving Activation Codes for Pseudonym Certificates Model. *SAE Int. J. Transp. Cybersecur. Priv.* **2020**, *3*, 57–77. [CrossRef]

12. Furtado, M.D.; Mushrall, R.D.; Liu, H. Threat analysis of the security credential management system for vehicular communications. In Proceedings of the 2018 IEEE International Symposium on Technologies for Homeland Security (HST), Crystal City, VA, USA, 2–3 May 2018; pp. 1–5.
13. Fernandes, B.; Rufino, J.; Alam, M.; Ferreira, J. Implementation and Analysis of IEEE and ETSI Security Standards for Vehicular Communications. *Mob. Netw. Appl.* **2018**, *23*, 469–478. [CrossRef]
14. Ghosal, A.; Conti, M. Security issues and challenges in V2X: A Survey. *Comput. Netw.* **2020**, *169*, 107093. [CrossRef]
15. Al-Shareeda, M.A.; Anbar, M.; Hasbullah, I.H.; Manickam, S. Survey of Authentication and Privacy Schemes in Vehicular ad hoc Networks. *IEEE Sens. J.* **2021**, *21*, 2422–2433. [CrossRef]
16. Hasrouny, H.; Samhat, A.E.; Bassil, C.; Laouiti, A. Misbehavior detection and efficient revocation within VANET. *J. Inf. Secur. Appl.* **2019**, *46*, 193–209. [CrossRef]
17. CAMP. Security Credential Management System Proof-of-Concept Implementation EE Requirements and Specifications Supporting SCMS Software Release 1.2.2. 2018. Available online: https://www.its.dot.gov/research_areas/cybersecurity/scms/SCMS-CV-Pilots-Documentation_26838136.html (accessed on 2 February 2022).
18. Verheul, E.; Hicks, C.; Garcia, F.D. Ifal: Issue first activate later certificates for v2x. In Proceedings of the 2019 IEEE European Symposium on Security and Privacy (EuroS&P), Stockholm, Sweden, 17–19 June 2019; pp. 279–293.
19. Liang, J.; Ma, M.; Yang, G.; Wang, H. Bac-Crl: Blockchain-Assisted Coded Caching Certificate Revocation List for Authentication in Vanets. *SSRN Electron. J.* **2022**. [CrossRef]
20. Didouh, A.; Labiod, H.; Hillali, Y.E.; Rivenq, A. Blockchain-Based Collaborative Certificate Revocation Systems Using Clustering. *IEEE Access* **2022**, *10*, 51487–51500. [CrossRef]
21. Perera, M.N.S.; Nakamura, T.; Hashimoto, M.; Yokoyama, H.; Cheng, C.M.; Sakurai, K. Certificate Management Scheme for VANETs Using Blockchain Structure. *Cryptography* **2022**, *6*, 20. [CrossRef]
22. Wang, Z.; Wang, H.; Wang, Y.; Yang, X. CLASRM: A Lightweight and Secure Certificateless Aggregate Signature Scheme with Revocation Mechanism for 5G-Enabled Vehicular Networks. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 1–20. [CrossRef]
23. Mistareehi, H.; Manivannan, D. A Low-Overhead Message Authentication and Secure Message Dissemination Scheme for VANETs. *Network* **2022**, *2*, 139–152. [CrossRef]
24. Whyte, W.; Weimerskirch, A.; Kumar, V.; Hehn, T. A security credential management system for V2V communications. In Proceedings of the 2013 IEEE Vehicular Networking Conference, Boston, MA, USA, 16–18 December 2013; pp. 1–8. [CrossRef]
25. Aiello, W.; Lodha, S.; Ostrovsky, R. Fast digital identity revocation. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 23–27 August 1998; Springer: Berlin/Heidelberg, Germany, 1998; pp. 137–152.