Dissertation

# On the Certificate Activation for V2X Communication

## (V2X 通信における証明書の有効化手法について)

Graduate School of
Natural Science & Technology
Kanazawa University

Division of
Electrical Engineering & Computer Science

| | | |
|---|---|---|
| Student ID No. | : | 1924042005 |
| Name | : | Jan Wantoro |
| Chief advisor | : | Prof. Masahiro Mambo |
| Date of Submission | : | June, 24, 2022 * |

# 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 uses many short valid period pseudonym certificates to meet the security and privacy requirements. However, this method has a difficulty to ensure 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 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 get benefits of efficient activation code distribution. The proposed scheme provides small communication resource usage in the V2X network with various channels option for delivering activation codes in a privacy preserved manner.

**Keywords:** Intelligent transportation systems; C-ITS; V2X; VANET; Security; Privacy

# Acknowledgements

I would like to express my gratitude and appreciation to my supervisor, Prof. Masahiro Mambo, who has provided guidance and input throughout the doctoral program. Thanks to all parties involved, this research can be carried out, especially for members of the Information Security Laboratory. I would also like to thank the Japanese Ministry of Education, Culture, Sports, Science, and Technology (MEXT) and the Japan International Cooperation Agency (JICA) for supporting full scholarships for my studies. Finally, I would like to thank my family, who supported me during the preparation of this dissertation.

# Contents

# List of Figures

# List of Tables

# Chapter 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. 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 the privacy-preservation, V2X should not make a detailed lifelong history of driver behavior for free by others, which centers around the concept of unlink-ability. So, eavesdroppers cannot quickly identify or track owners of unrevoked vehicle certificates.

Many groups of research designed security solutions for V2X based on the PKI [3]. For privacy protection purposes, they apply pseudonym certificates with a reasonably limited validity period which needs to be changed regularly [2]. The pseudonym certificates are used to sign V2X messages like the basic safety message that is periodically transmitted by vehicles or roadside units. every 10 seconds.

## 1.1 Background

Revocation process is the biggest weakness of a PKI scheme [4]. 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, so it is sufficient for long-term usage, e.g., for three years. In that case, revoking the certificate will overfill certificate revocation lists (CRL) very quickly [5]. To solve this problem, the United States (US) and Europe (EU) take the following different approaches. The development of V2X PKI for cooperative intelligent transportation systems (C-ITS) in the EU decides to provide certificates only for thee months of use [6].

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 [7]. Conversely, the development of V2X PKI in the US, called the security credential management system (SCMS), decides 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 CRL. It is still a burden on the system, especially on the fact that the link seed of 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 CA while reducing costs caused by large CRL is to use the activation codes technique [8]. 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 solution that uses this method is the ACPC[9]. 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 phone, reduces the V2X PKI infrastructure burden. It contrasts with periodic pseudonymous certificate issuance as described in European Telecommunications Standards Institute (ETSI) [10], which requires the vehicle to establish and maintain a secure connection to 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. Contrarily, vehicles are mobile devices with intermittent wireless networks. Moreover, the vehicles are inactive when it stays in the garage or parking lot. This situation makes the vehicles cannot receive the activation code broadcast, so the vehicles are 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 to show 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 [9]. 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 done by the binary hash tree based certificate access management (BCAM) scheme [7]. 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 [11]. The DR is the most efficient scheme but cannot preserve privacy requirements. So, the activation code for pseudonym certificate (uACPC) [12] 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.

## 1.2 Contribution

1. We propose a scheme that take advantage of cache devices such as the RSU based on the ACPC design to achieve efficiency of activation code distribution on V2X while providing the privacy preservation.
2. 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.
3. Our scheme provides a different `CID` for each activation period to avoid vehicle tracking during the unicast distribution model.
4. Our scheme can benefit from the unicast distribution model for efficient activation code distribution.
5. We propose an efficient and flexible activation code distribution strategy to shorten the abuse period by setting a shorter certificate activation period. That is, shortening the abuse period with a smaller communication cost than the previous schemes.

## 1.3 Dissertation Organization

The rest of this dissertation is organized as follow. Chapter 2 we introduce the background of this study, such as V2X and its security mechanisms, vehicullar public key infrastructure (VPKI), and the activation code technique, describes related work that has been done so far to reduce the size and improve distribution efficiency of activation code. Chapter 3 explains how we design our proposed scheme to meet our goal. Then we shows and discusses the result of our schemes as well as the comparison in Chapter 3.3 and conclude our work in Chapter 5.

# Chapter 2

# Preliminaries

## 2.1 V2X Communication

V2X is a vehicle communication system that combines other, more specific types of communication such as vehicle to vehicle (V2V), vehicle to infrastructure (V2I), vehicle to network (V2N), vehicle to pedestrian (V2P), vehicle to device (V2D) as ilustrated in Figure 2.1. The exchange of information and communication between vehicles and the roadside infrastructure is the basis of ITS. These communications will help optimize traffic flows, reduce congestion, cut accident numbers, and minimize emissions.

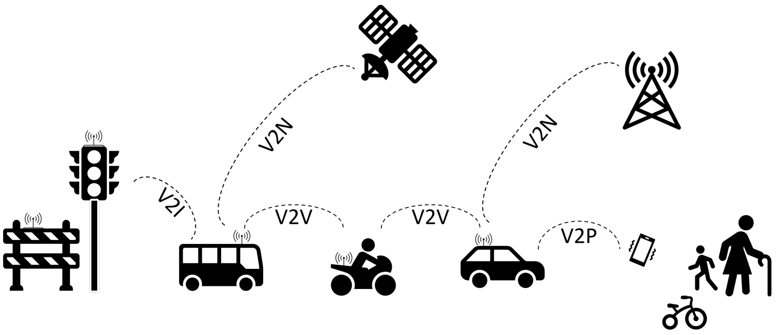


Figure 2.1: V2X Communication Types

Many applications can be applied on top of V2X technology, from an environment-related applications, mobility, road weather, and safety application. The following are well-known examples of applications that utilize V2X technology:

- Platooning

  Platooning uses cooperative adaptive cruise control in a series of vehicles to improve traffic flow stability and safely allow short headways to obtain mobility and fuel efficiency benefits.

- Safety Warning

  Wireless Connectivity allows cars to be continuously aware of each other, so when one car brakes suddenly, cars several yards behind the vehicle get a safety warning before they get too close.

- Traffic Signal

  Traffic signals are a vital part of the connected vehicle environment. They will help to prevent crashes by sharing messages between all nearby vehicles, infrastructure, and even pedestrian cell phones.

There are two types of V2X communication technology Wireless LAN (WLAN)-based and cellular-based. The WLAN-based V2X specification based on IEEE 802.11p [13] that refer to the dedicated short range communications (DSRC). The V2X communication using WLAN technology can be done directly without needing other communication infrastructure, the vehicles can form an ad-hoc network. Before being further developed for V2X, DSRC was widely used for electronic toll collection or road pricing.

The cellular-based V2X communication is named as cellular V2X (C-V2X) to distinguish it from WLAN-based V2X. The C-V2X is based on LTE technology and designed to operate V2V, V2I, and V2N. The PC5 interface is defined to support direct communication on V2V and V2I [14].

The vehicles will broadcast the basic safety message (BSM) up to ten times per second to support V2X safety applications. The BSM include the senders' time, position, speed, path history, and other relevant information and are digitally signed. The receiver evaluates each message, verifies the signature, and then decides whether a warning must be shown to the driver. The correctness and reliability of BSMs are critical as they directly affect the effectiveness of safety applications based on them.

## 2.2 V2X Security

Secure V2X communications is to ensures that only trustworthy vehicle and roadside infrastructure communicate. In addition, the V2X communication technology must protect the driver's privacy to prevent the possibility of tracking a specific vehicle. To prevent an attacker from inserting false messages, the sending vehicles digitally sign each BSM, and the receiving vehicles verify the signature before acting on it. This approach has been recommended by many different studies of the system in both EU and US [2].

If there is no security system on V2X, one thing that can happen is a traffic jam attack. Hackers make fake cars, and fake cars send a lot of fake signals. The traffic light reaches the heavy traffic and turns green. All other cars have to wait, which causes traffic jams [3].

The principle of V2X communication security is based on signed messages using public key certificates. In EU and the US, ETSI ITS, and Institute of Electrical and Electronics Engineers (IEEE) have both respectively defined PKI architectures to secure all V2V and V2I communications. For privacy protection purposes, they apply pseudonym certificates with a reasonably limited validity period and need to be changed regularly. All valid V2X devices are given a long-term enrolment certificate during production. The enrolment certificate is used to download short-term pseudonym certificates from the CA. Vehicle send out a BSM to tell other vehicle and roadside equipment where they are. The BSM is signed using one of the valid short-term pseudonym certificates. To protect driver′s privacy, each car later selects from the batch of concurrently valid short-term pseudonym certificate and changes frequently while driving.

V2X PKI is an adapted form of PKI used to achieve the key management and security services in V2X. Certificate generation and revocation is one of the primary functions of V2X PKI. It is distinguished from a traditional PKI in several aspects. The two most important aspects being its size (i.e., the number of devices that it supports) and the balance among security, privacy, and efficiency. At its full capacity, it will issue approximately 300 billion certificates per year for 300 million vehicles.

## 2.3 Certificate Revocation

The whole process of making invalid an issued certificate of the compromised vehicle is called revocation[15]. Revocation information is the information that can be used to determine whether a vehicle has been revoked. In general, there are two methods to indicate revocation information: black list and white list. The revocation mechanism for vehicular networks should take into consideration three goals in the following:

- The revocation information should be distributed to vehicles as soon as possible, i.e., the revocation vulnerability window should be small.
- The overheads caused by revocation information distribution should be as low as possible.

- The usage of revocation information should be as efficient as possible. It is better that the revocation checking process does not cause high latency.

Authorized vehicle should be revoked if the vehicle become compromised. Certificate revocation is used for revoking the malicious nodes and terminate their access rights to the network. Vehicle wishes to obtain the latest revocation information as timely as possible such that it can minimize the risk of being attacked by the compromised vehicle. It is necessary to take the delay constraint into account when design revocation mechanism, because vehicular networks are delay-sensitive.

The revocation mechanism for vehicular networks should take into consideration three goals in the following:

- The revocation information should be distributed to vehicles as soon as possible.
- The overheads caused by revocation information distribution should be as low as possible.
- The usage of revocation information should be as efficient as possible.
- It is better that the revocation checking process does not cause high latency.

## 2.4 Standard Body Approach for Certificate Revocation

The standards and interoperability are critical in V2X. There is a directive mandating interoperable V2X between member states [16]. Notably, in the US and EU, there is convergence across all standards upon the elliptic curve digital signature algorithm (ECDSA) signature scheme [17]. 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 [18]. Privacy in V2X PKI will manage 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 certificates revocation. It will lead the CRL entry size to grow too large, which also affects the process of message verification [4].

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 like cooperative awareness messages, because it is a kind of real-time message type that is delay sensitive. As the PKI architecture in general, how to effectively update the CRLs entries is also a problem in V2X PKI, even more complicated. 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 revoked pseudonym certificate is undetected during message certificates verification.

There are two different approaches that US and EU standards use to deal with pseudonym certificate revocation problems. The ETSI ITS standard [6] decided to provide only a limited number of pseudonym certificates for a short period (2-3 months), consequently the vehicle periodically connects to RA and gets 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 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 IEEE and ETSI are not defined yet [19].

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 to a single device to avoid insider attacks on end-users privacy. It has defined the SCMS pilot project [20] 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) uses to link every short-term certificate belonging to the vehicle. Only one key per vehicle to revoke 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 [21], 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.

## 2.5 SCMS

SCMS [2] is a PKI designed to secure V2X messages e.g., BSM. Just like PKI in general, the primary purpose of SCMS is to secure messages to provide reliable communication. In simple terms, SCMS must first make sure that the sender of the message is a legally registered entity. The receiver needs to ensure that the message is the original message and that there are no changes during transmission. However, SCMS is used to support enormous capacities. It can issue up to 300 billion certificates annually, enough to keep up to 300 million vehicles. Besides that, SCMS must also maintain user privacy while using these certificates. The architecture overview of SCMS is in Figure 2.2

In the SCMS model, a certificate was valid for a specific 5-minute period, which would correspond to 105,120 certificates per year [2]. Given the connectivity constraints, in full deployment a device may need up to 3 years' worth of certificates, which would amount to more than 300,000 certificates. This approach is prohibitively expensive in terms of automotive-grade storage requirements on

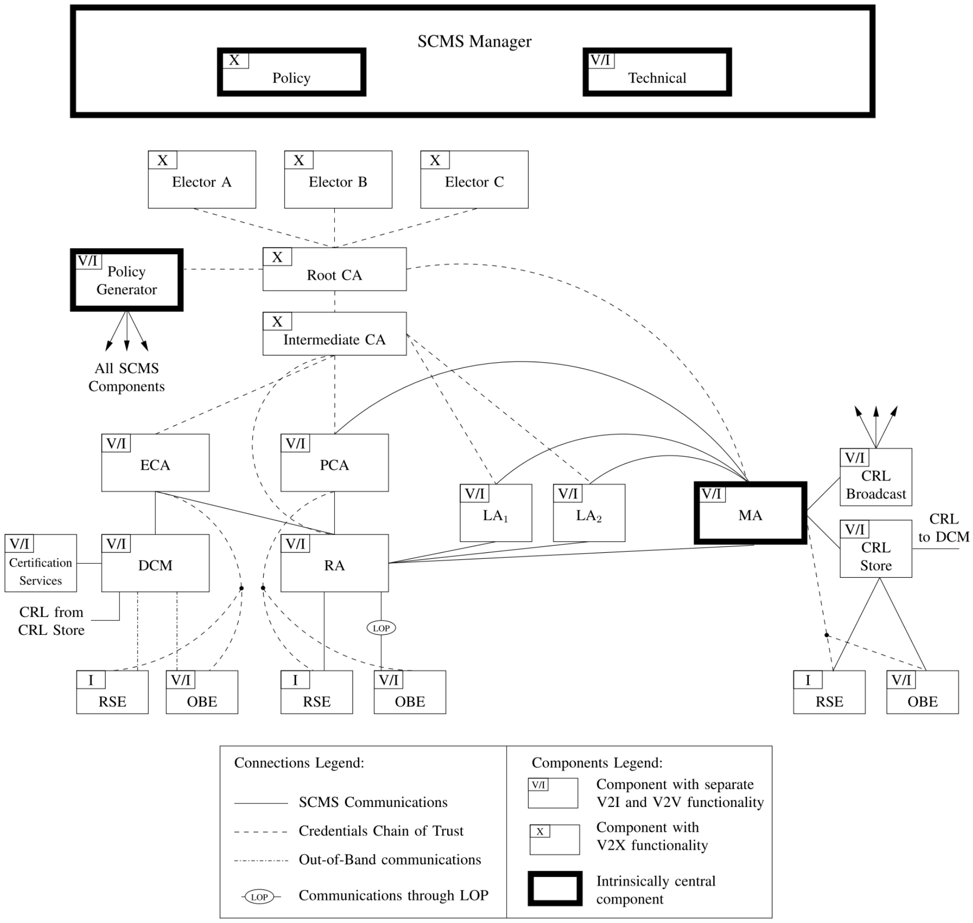


Figure 2.2: SCMS architecture overview (source: [2])

the device.

The Misbehavior Authority (MA) revokes and blacklists a device if it determines during misbehavior investigation that the device was indeed misbehaving. The MA adds CertIDs (8 bytes) of all non-expired certificates to the CRL. The size of the CRL grows linearly with the number of revoked entities. The assumption is that all original equipment manufacturer (OEM) will provide at least enough storage for 10,000 entries, which translates to a file size of approximately 400 KB. Unfortunately, though, SCMS original revocation mechanism can lead to large CRL, which in turn impacts the bandwidth usage and processing overhead of the system.

## 2.6 IFAL

The IFAL [8], [21] scheme is a practical improvement upon the ETSI ITS standard V2X architecture as shown in Figure 2.3. The IFAL scheme pre-issues vehicles with a lifetime supply of pseudonym certificates during manufacture divides the certificates into epochs and then periodically issues activation codes that enable a vehicle to derive pseudonym signatures during an epoch. By removing the need for CRL, IFAL offers improved verification latency over the previous proposals in the ETSI ITS standard.

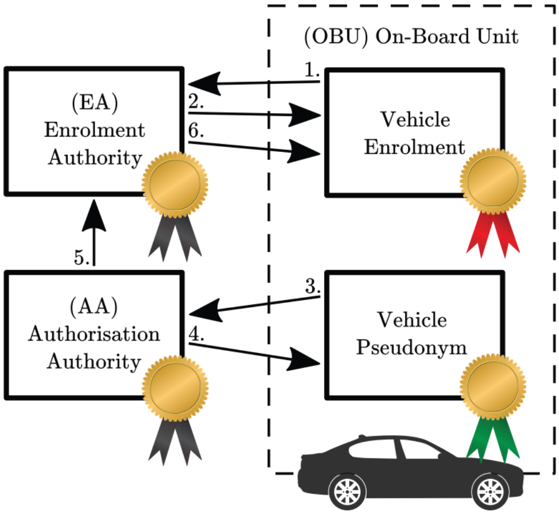


Figure 2.3: Simplified IFAL PKI model (source: [21])

1. The vehicle owner registers ID and public key value with the EA.
2. The EA provides the vehicle with an enrolment certificate and a unique uid value.
3. The vehicle provides the enrolment certificate, its uid and an activation code distribution channel specification to the AA.
4. The AA provides the vehicle with a pseudonym certificate file.
5. The AA periodically sends activation codes for all entitled vehicles to the EA.
6. The EA distributes activation codes by relating the uid to a vehicle identity and a distribution channel specification.

IFAL activation codes are much smaller than the corresponding pseudonym certificates and therefore facilitate a much broader range of vehicle connectivities. Several activation codes fit within a single short message sevice (SMS) message and may even be entered manually during vehicle servicing. Misbehaving vehicles are removed from the scheme by refusing to issue further activation codes and therefore denying vehicles the capability to sign messages.

## 2.7 BCAM

In BCAM [7], vehicles are provisioned at the start of their lifetime with all the certificates they will need as in the SCMS. The corresponding private keys are generated on the vehicle so that no other entity knows apart from the vehicle itself. When the certificates and the corresponding private key reconstruction values are provided to the vehicle, they are encrypted, and the keys to decrypt them are only made available to the vehicles shortly before the validity periods of those certificates.

The SCMS diagram modified to support BCAM, is shown in Figure 2.4. CAM has been added as a new component in the SCMS architecture. Then the BCAM changed the two SCMS components associated with CRL renamed to reflect their new roles. CRL Generator changed to Revocation Generator (RG), and CRL Broadcast changed to Certificate Access Broadcast (CAB)

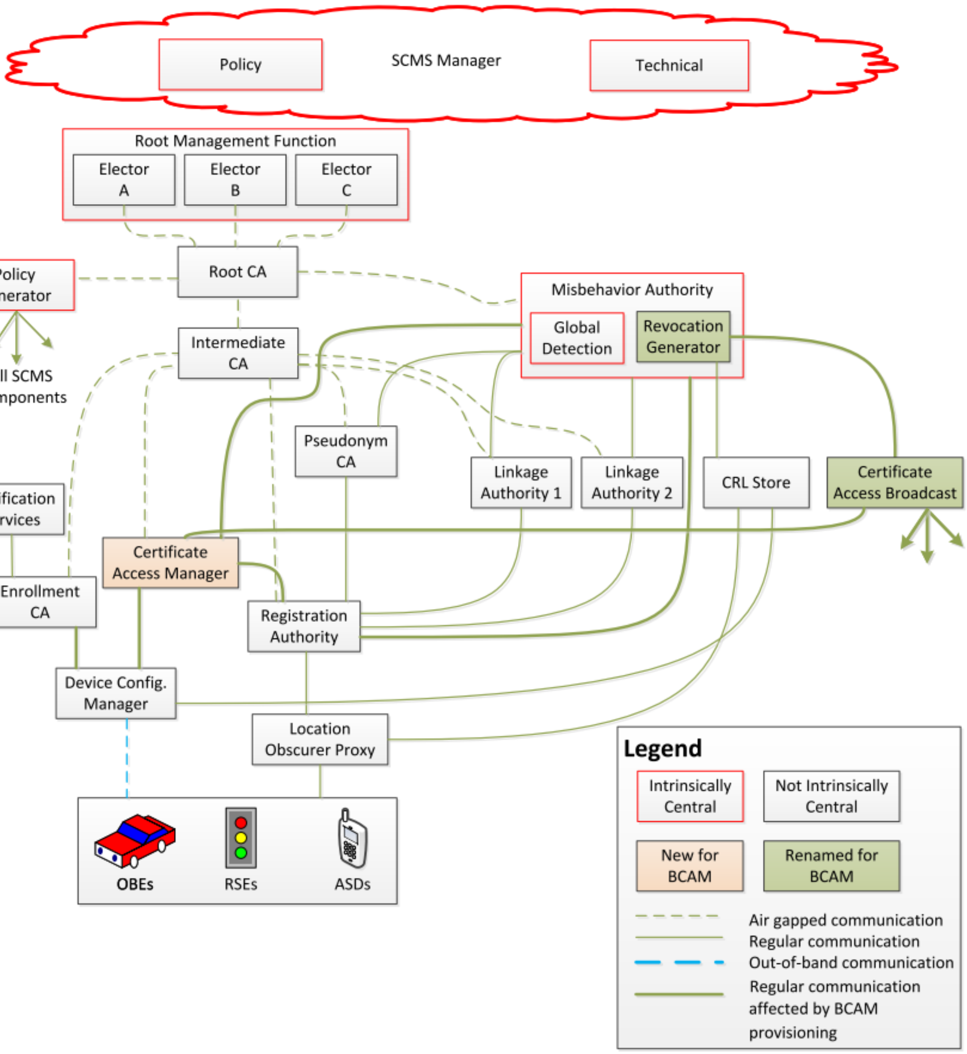


Figure 2.4: SCMS with Certificate Access Manager (source: [7])

The pseudonym certificate model (i.e., certificate validity, number of concurrently valid certificates, etc.) is unchanged and follow the current SCMS design. This, in turn, means that the SCMS use cases of misbehavior reporting and global misbehavior detection are also unaffected by the BCAM system and should work exactly like the current system.

Revocation is modified, compromised vehicles are prevented from participating in the V2X system by not giving them the necessary keys for decrypting the certificates (and the corresponding private key reconstruction values).

## 2.8 ACPC

To avoid high CRL growth while maintaining the performance improvements associated with butterfly key derivation, ACPC [9] builds on the IFAL [8] 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 [7] 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 doesn't know that a group of 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. Also, 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 [11]. The ACPC activation code takes only 16 bytes, 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 doesn't 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 CRL or the frequent provision of pseudonym certificates.

Reducing bandwidth costs between infrastructure and vehicles on ACPC schemes is done 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 done 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 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.

## 2.9 Unicast Distribution of Activation Code and Its Privacy Issue

Simplicio et al. [11] and Cunha et al. [12] 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 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, moreover, if the communication is done 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 [11]. 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 well 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 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 [12] 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 pseudorandom 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 sent 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.

## 2.10 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 (128bits) than its predecessor BCAM (256bits)[9]. 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 2.5.

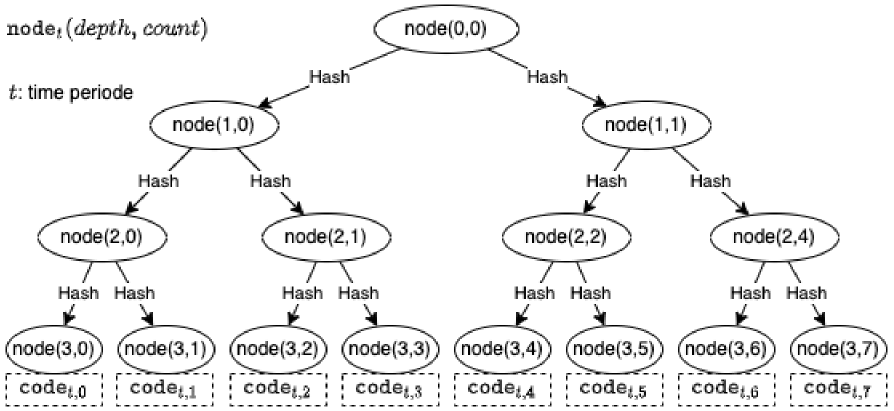


Figure 2.5: Binary Tree Activation Code Generation

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 $\tau$ time range. The desired security level is determined by the bit string length $k$ as in equation 2.1. Then the CAM determines all the values of the $\texttt{node}_t$ in the binary hash tree construction (equation 2.2), each node is computed from its upper level node concatenated by a unique suffix security string $I$ (equation 2.3), which is 104 bit length. It is designed to support 40-bit long $\texttt{CID}$ for $2^{16}$ time periods, which means more than 1200 years if the time periods are 1 week.

$$\texttt{node}_t(0,0) = \{0,1\}^k \tag{2.1}$$

$$\texttt{node}_t(depth, count) = Hash(\texttt{node}_t(depth-1, \lfloor count/2 \rfloor)\|I) \tag{2.2}$$

$$I = (\texttt{cam\_id}\|t\|dept\|count) \tag{2.3}$$

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.

# Chapter 3

# Efficient and Flexible Certificate Activation

## 3.1 Introduction

Simplicio et al. [11] and Cunha et al. [12] 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 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, moreover, if the communication is done 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 [11]. 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 well 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 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 [12] 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 pseudorandom 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 sent 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.

For convenience of the reader, we define the symbols and notations used in Table 3.1. Since we built it on top of ACPC, most notations borrow from ACPC with some additions.

Table 3.1: General notation and symbols

| Symbol | Meaning |
|---|---|
| `node` | A binnary 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,<br>dedicated to the `CID` encryption and decryption |
| $\hat{E}, \hat{e}$ | Public and private cocoon encryption keys,<br>dedicated to the `pkg` encryption and decryption |
| $\hat{S}, \hat{e}$ | Public and private cocoon signature keys that paired with $\hat{E}$ and $\hat{e}$ |
| $f_2, f_3$ | Pseudorandom function |
| $f_4$ | Random choice function |
| $\beta$ | Number of cocoon keys in pseudonym certificates batch |
| $t$ | Pseudonym certificate time perod |
| $\tau$ | Number of time period in pseudonym certificates batch |
| $\alpha$ | Number of activation time period |
| $\sigma$ | Number of valid certificates each period |
| `cert` | A pseudonym certificate |
| `pkg` | An encrypted pseudonym certificate |
| `CID` | Code identity or binnary 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 bitstring *str* with key $\kappa$ |
| $Dec(str, \kappa)$ | Decryption of bitstring *str* with key $\kappa$ |
| $n_t$ | Number of total vehicle or number of total binnary tree leaf |
| $n_r$ | Number of revoked vehicle or number of marked (as revoked)<br>binnary tree leaf |
| $n_b$ | Number of the binnary tree node that distributed |
| $\|str\|$ | Length of bit-string *str*, in bit |

## 3.2 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 2.8. In our proposed scheme, one vehicle uses different identities for each activation period. In other word, 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 `VID`s 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 each other. It is become 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. And 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 get 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 did not get 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.

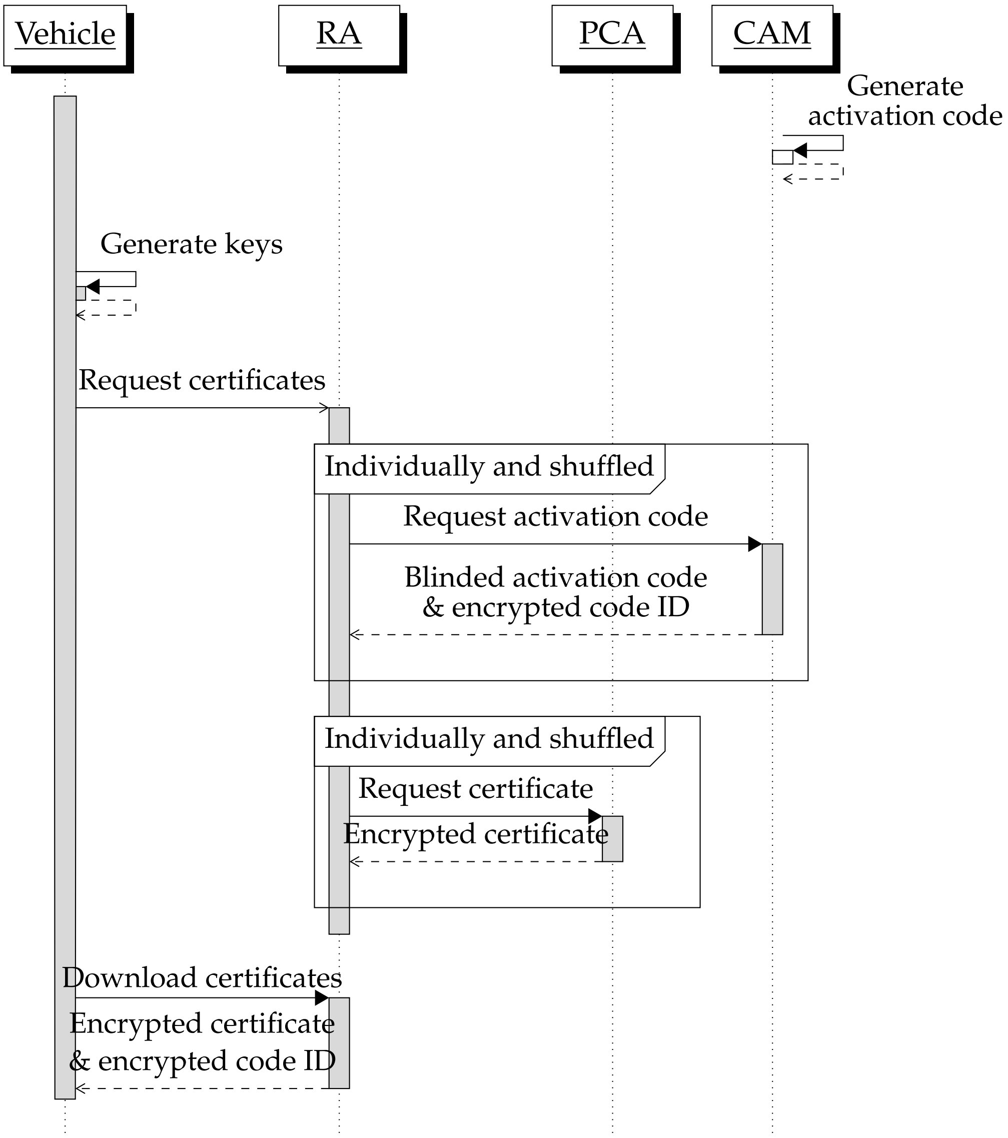
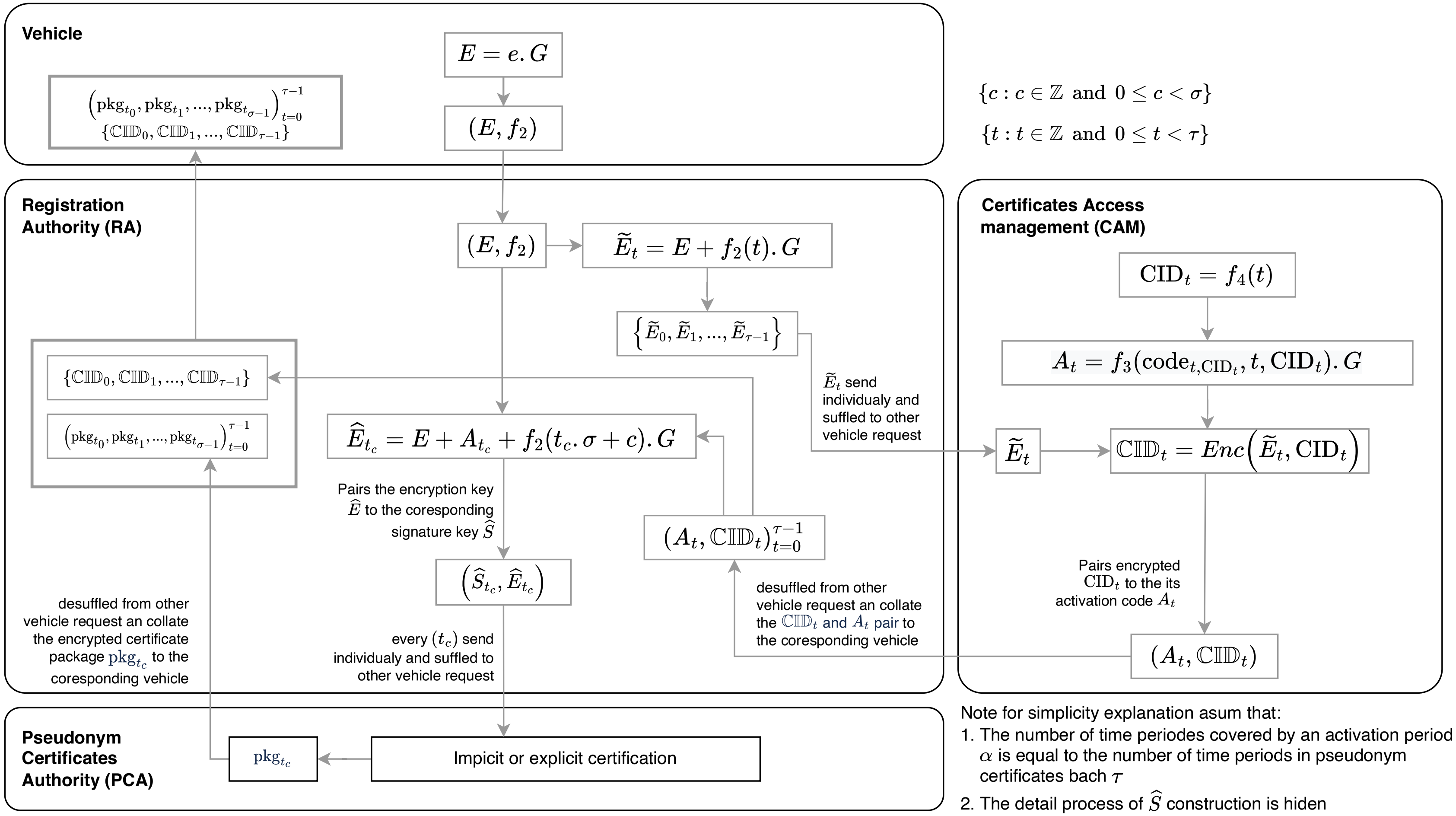


Figure 3.1: Pseudonym certificate issuing phase

### 3.2.1 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 2.10. We choose this construction because they have a small activation code that can benefit the distribution process. After all the activation code construction in the binary tree form are complete, vehicles can start registering to get their respective pseudonym certificates. The pseudonym certificate issuing phase can be described as shown in Figure 3.1. Then, for the details of the process for each entity involved, it can be seen in Figure 3.2.

The vehicle starts by supplying a randomly selected *caterpillar* private key $s$


Vehicle
$E = e.G$
$(E, f_2)$
$\left(\mathrm{pkg}_{t_0}, \mathrm{pkg}_{t_1}, ..., \mathrm{pkg}_{t_{\sigma-1}}\right)_{t=0}^{\tau-1}$
$\{\mathbb{CID}_0, \mathbb{CID}_1, ..., \mathbb{CID}_{\tau-1}\}$
Registration Authority (RA)
$(E, f_2)$
$\widetilde{E}_t = E + f_2(t).G$
$\left\{\widetilde{E}_0, \widetilde{E}_1, ..., \widetilde{E}_{\tau-1}\right\}$
$\widetilde{E}_t$ send individualy and suffled to other vehicle request
$\{\mathbb{CID}_0, \mathbb{CID}_1, ..., \mathbb{CID}_{\tau-1}\}$
$\left(\mathrm{pkg}_{t_0}, \mathrm{pkg}_{t_1}, ..., \mathrm{pkg}_{t_{\sigma-1}}\right)_{t=0}^{\tau-1}$
$\widehat{E}_{t_c} = E + A_{t_c} + f_2(t_c.\sigma + c).G$
Pairs the encryption key $\widehat{E}$ to the coresponding signature key $\widehat{S}$
$(A_t, \mathbb{CID}_t)_{t=0}^{\tau-1}$
$\left(\widehat{S}_{t_c}, \widehat{E}_{t_c}\right)$
desuffled from other vehicle request an collate the encrypted certificate package $\mathrm{pkg}_{t_c}$ to the coresponding vehicle
every $(t_c)$ send individualy and suffled to other vehicle request
desuffled from other vehicle request an collate the $\mathbb{CID}_t$ and $A_t$ pair to the coresponding vehicle
Certificates Access management (CAM)
$\mathrm{CID}_t = f_4(t)$
$A_t = f_3(\mathrm{code}_{t,\mathrm{CID}_t}, t, \mathrm{CID}_t).G$
$\widetilde{E}_t$
$\mathbb{CID}_t = Enc\left(\widetilde{E}_t, \mathrm{CID}_t\right)$
Pairs encrypted $\mathrm{CID}_t$ to the its activation code $A_t$
$(A_t, \mathbb{CID}_t)$
Pseudonym Certificates Authority (PCA)
$\mathrm{pkg}_{t_c}$
Impicit or explicit certification

$\{c : c \in \mathbb{Z} \text{ and } 0 \leq c < \sigma\}$

$\{t : t \in \mathbb{Z} \text{ and } 0 \leq t < \tau\}$

Note for simplicity explanation asum that:
1. The number of time periodes covered by an activation period $\alpha$ is equal to the number of time periods in pseudonym certificates bach $\tau$
2. The detail process of $\widehat{S}$ construction is hiden

Figure 3.2: Pseudonym Certificates Issuing Diagram

and $e$ with the corresponding public *caterpillar* key $S = s \cdot G$ and $E = e \cdot G$. The key $s$ and $e$ are for signing and encryption, respectively. It also picks up two random seeds to initialize the pseudorandom functions $f_1$ and $f_2$ for later butterfly key expansion constructs, as was done 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 $\beta$ certificates divided into several $\tau$ activation periods, where $\sigma$ is the number of certificates per period.

$$\beta = \tau \cdot \sigma \tag{3.1}$$

Since the $S$ and $f1$ parts are unchanged in our construction and remain consistent with the original SCMS design, their process details do not iclude in the diagram shown in Figure 3.2 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 public cocoon encryption key $\hat{E}$ to encrypt the certificate, first, it creates a public cocoon encryption key $\tilde{E}_t$ (equation 3.2) 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 [22].

$$\tilde{E}_{t_c} = E + f_2(t) \cdot G \tag{3.2}$$

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

$$\texttt{CID}_t = f_4(t) \tag{3.3}$$

$$\texttt{code}_t = \texttt{node}_t(|\texttt{CID}|, \texttt{CID}) \tag{3.4}$$

$$A_t = f_3(\texttt{code}_t, \texttt{CID}_t, t, \texttt{CID}_t) \cdot G \tag{3.5}$$

$$\mathbb{CID}_t = Enc(\texttt{CID}, \tilde{E}_t) \tag{3.6}$$

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 3.7. Then, $\hat{E}_t$ is used in pairs with the public *cocoon* keys $\hat{S}_t$ to generate a pseudonym certificate by PCA as done 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 $0 < c \leq \sigma$.

$$\hat{E}_{t_c} = E + A_{t_c} + f_2(t_c \cdot \sigma + c) \cdot G \tag{3.7}$$

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 no 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 it decrypting the $\mathbb{CID}_t$ as a reference to get the appropriate code for its certificates.

### 3.2.2 Activation Code Usage

The stages of distribution and the activation code usage by vehicles can be seen in Figure 3.3. In order for the vehicle able 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 equation 3.8 and 3.9. 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

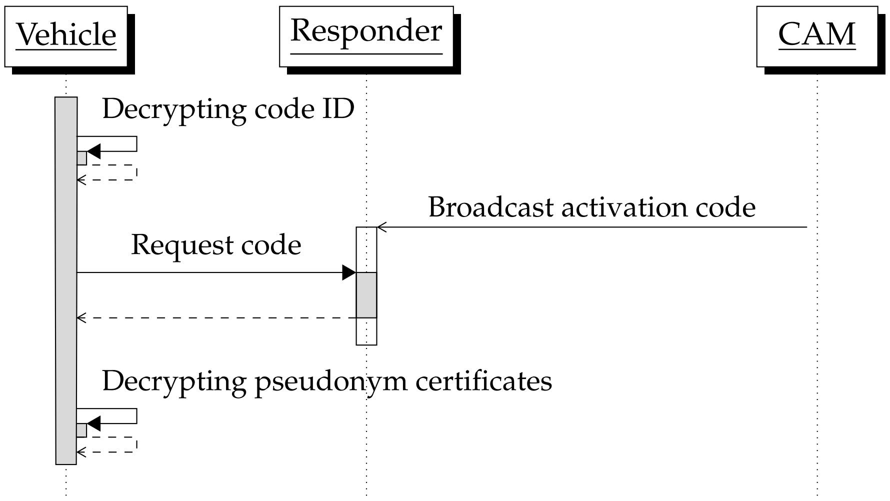


Figure 3.3: Activation code issuing and usage phase

when request for specific activation code to the responder.

$$\tilde{e}_t = e + f_2(t) \tag{3.8}$$

$$\texttt{CID}_t = Dec(\mathbb{CID}_t, \tilde{e}_t) \tag{3.9}$$

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 3.10). Then, the vehicle decrypts its pseudonym certificate using the $\hat{e}_t$. The complete diagram for the certificate activation can be seen in Figure 3.4. With active pseudonym certificates, vehicles can use it for message authentication on required V2X applications.

$$\hat{e}_t = e + f_3(\texttt{code}_{t,\texttt{CID}_t}) + f_2(t_c \cdot \sigma + c) \tag{3.10}$$

$$\texttt{cert}_{t_c} = Dec(\texttt{pkg}_t, \hat{e}_t) \tag{3.11}$$

### 3.2.3 Activation Code Distribution Scenarios

All vehicles require an activation code to use their certificate in each period. In our scheme, the activation code is able to 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 done in a unicast communication manner, i.e., the vehicle will ask the RSU, cellular tower, or public cloud to get its activation code, see

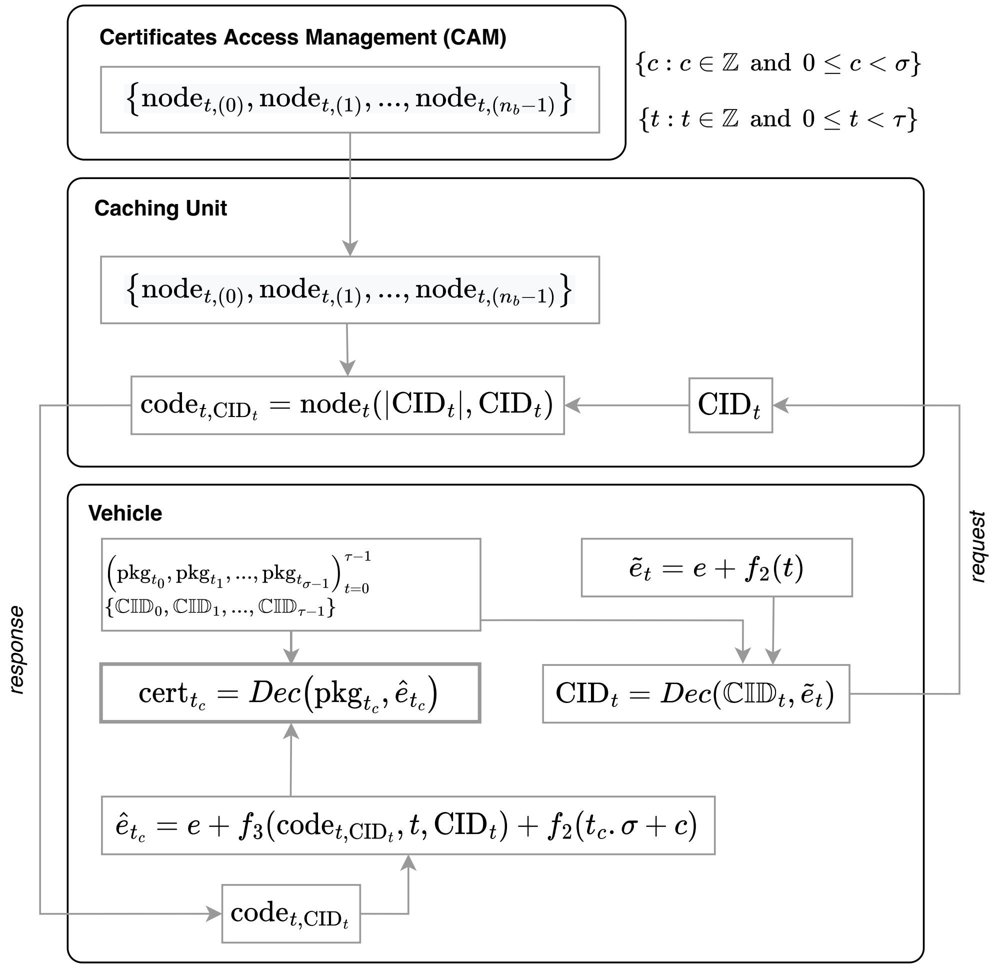

Certificates Access Management (CAM)
$\{\text{node}_{t,(0)}, \text{node}_{t,(1)}, ..., \text{node}_{t,(n_b-1)}\}$
$\{c : c \in \mathbb{Z} \text{ and } 0 \le c < \sigma\}$
$\{t : t \in \mathbb{Z} \text{ and } 0 \le t < \tau\}$
Caching Unit
$\{\text{node}_{t,(0)}, \text{node}_{t,(1)}, ..., \text{node}_{t,(n_b-1)}\}$
$\text{code}_{t,\text{CID}_t} = \text{node}_t(|\text{CID}_t|, \text{CID}_t)$
$\text{CID}_t$
request
response
Vehicle
$(\text{pkg}_{t_0}, \text{pkg}_{t_1}, ..., \text{pkg}_{t_{\sigma-1}})_{t=0}^{\tau-1}$
$\{\mathbb{CID}_0, \mathbb{CID}_1, ..., \mathbb{CID}_{\tau-1}\}$
$\tilde{e}_t = e + f_2(t)$
$\text{cert}_{t_c} = Dec(\text{pkg}_{t_c}, \hat{e}_{t_c})$
$\text{CID}_t = Dec(\mathbb{CID}_t, \tilde{e}_t)$
$\hat{e}_{t_c} = e + f_3(\text{code}_{t,\text{CID}_t}, t, \text{CID}_t) + f_2(t_c.\sigma + c)$
$\text{code}_{t,\text{CID}_t}$

Figure 3.4: Certificate Activation Diagram

Figure 3.5. Then the V2X network only uses 40 bits `CID` for upload and 16 bytes (128bits) for downloads per vehicle activation period.

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 get the code through communication media such as email or short message service (SMS). It is also possible that users get a 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.

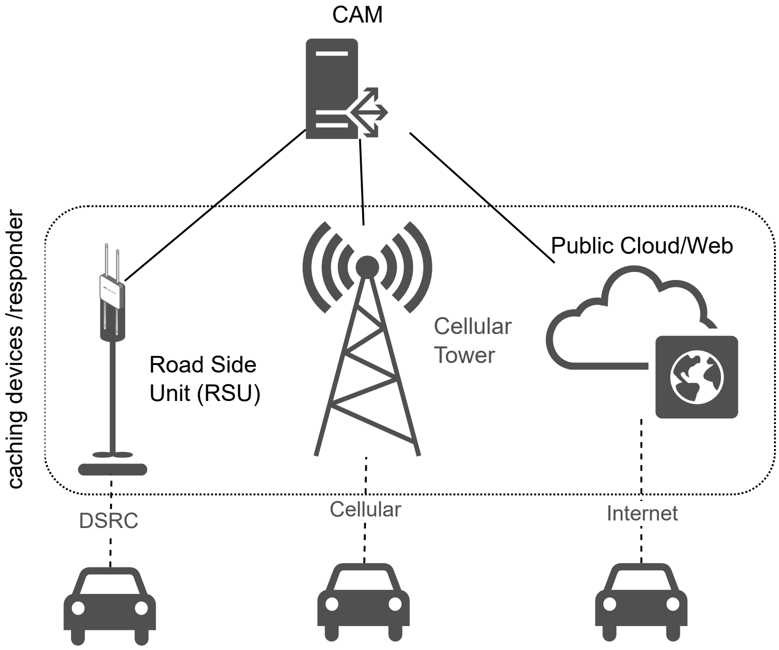


Figure 3.5: Caching strategy distribution

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. 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 are 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 get an activation code 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 [8]. 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 DSRC technology via the RSU along the road. The RSU then forwarded it to the internet network so the vehicle can be communicated 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 get 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 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 by other applications. The efficient bandwidth usage by V2X PKI is very beneficial for the V2X network.

To get 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 3.6. The closest unit to the vehicle on the road is the RSU. If the RSU becomes a responder activation code, it brings the activation code easy access by the vehicles.

With a different `CID` for each period as described in 3.2.1, even if the certificate authority does not control the responder, the vehicle can request an activation code to the responder without worrying about it privacy. The untrusted responder is hard to track the vehicle path base 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

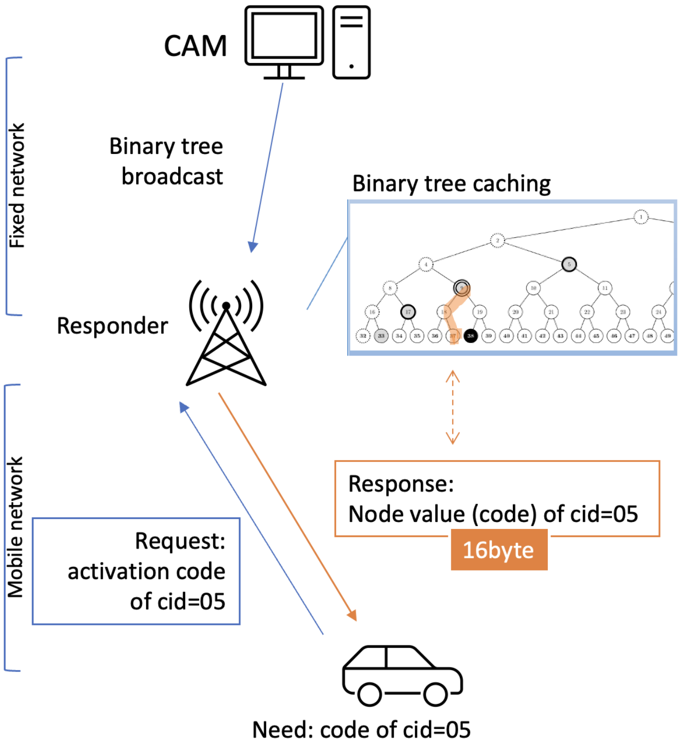


Figure 3.6: Unicast Distribution

achieved in a minimum size because the activation code sent from the responder to the vehicle is only one code (16bytes). Moreover, the cache unit utilization reduces certificate the authority burden and provides more alternatives for the vehicles to get their activation code.

## 3.3 Performance and Discussion

### 3.3.1 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.

### 3.3.2 Privacy Protection: Different Code Identity in Each Activation Period

On the unicast distribution, the vehicles can request the activation code by showing its CID, so the RSU can immediately respond to the correct activation code. The ACPC has a privacy issue when using this unicast model, so they tried to solve this issue by increasing the crowd size privacy level [11]. 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 [12]. The different CID technique inspires 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.

### 3.3.3 Privacy Protection: Hiding the Code Identity From V2X PKI entity

The CID is used by the vehicle to request their 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 do to the request for 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 he 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.

### 3.3.4 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's 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 $1 \leq n_r \leq n_t/2$ [23]. The number of variable node $v_n$ on VSS is dependent on vehicle request security level [11]. 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 3.2, 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 $16byte * n_b = 1.420Mbyte$ . The enormous download size from CAM to RSU is 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 bytes and 5 bytes of the epoch identifier, with an additional 7 bytes of the code identifier [8]. So, the IFAL activation code for all unrevoked vehicles in total is $27byte * (n_t - n_r) = 29.686.679Mbyte$ .

The storage required by the RSU to keep activation code is equal to activation code download size from CAM to RSU. The RSU must store $27(n_t - n_r) = 29.686.679Mbyte$ activation code for IFAL. With such a large size for one activation period, it is difficult to expect IFAL to use a scenario whith 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 $16n_b = 1.420Mbyte$.

Table 3.2: Performance cost under example parameters

| | IFAL | ACPC | uACPC | FSS | VSS | Our scheme |
|---|---|---|---|---|---|---|
| ***CAM to RSU:*** | | | | | | |
| Download (Mbyte) | 29.686.679 | 1.420 | 1.420 | 1.420 | 1.420 | 1.420 |
| ***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 | 1.420 | 1.420 | 1.420 | 1.420 | 1.420 |

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 |

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 that the vehicle activation code is derived from it. Changes the number of revoked vehicles or active vehicles have no effect on upload and download sizes between RSU and vehicle. Meanwhile, there is 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 $16n_b = 1.420 Mbyte$. 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 than the other schemes.

### 3.3.5 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 $\tau$. Assuming that the pseudonym certificate file size $S_{pc}$ is similar for all schemes with roughly 128 bytes. To simplify the calculation let's say that one certificate is sufficient to cover one $t$, the total certificate size is $S_{pc} * \tau$. Total activation period $\alpha$ is the total period $a$ that every $a$ covers some certificates batch. Each certificate has a $t$ validity period, and the entire validity period $\tau$ 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 $t = 5$ minutes 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 vehicle has to store all CID which is 40 bits per activation period.

As shown in Figure 3.7, 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 is prepared for ten 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 no significant difference compared to other systems. So it is no restriction in storage usage of vehicle OBU.

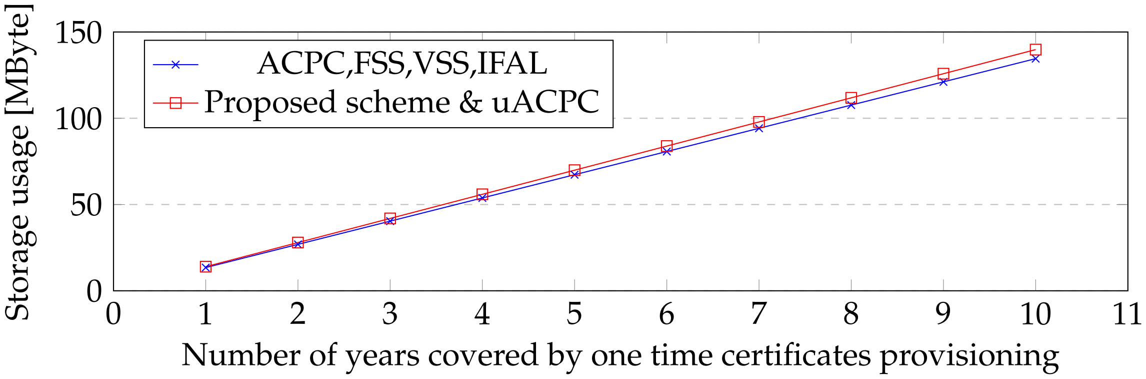


Figure 3.7: Storage usage in the vehicle

### 3.3.6 Reducing Vulnerability Window

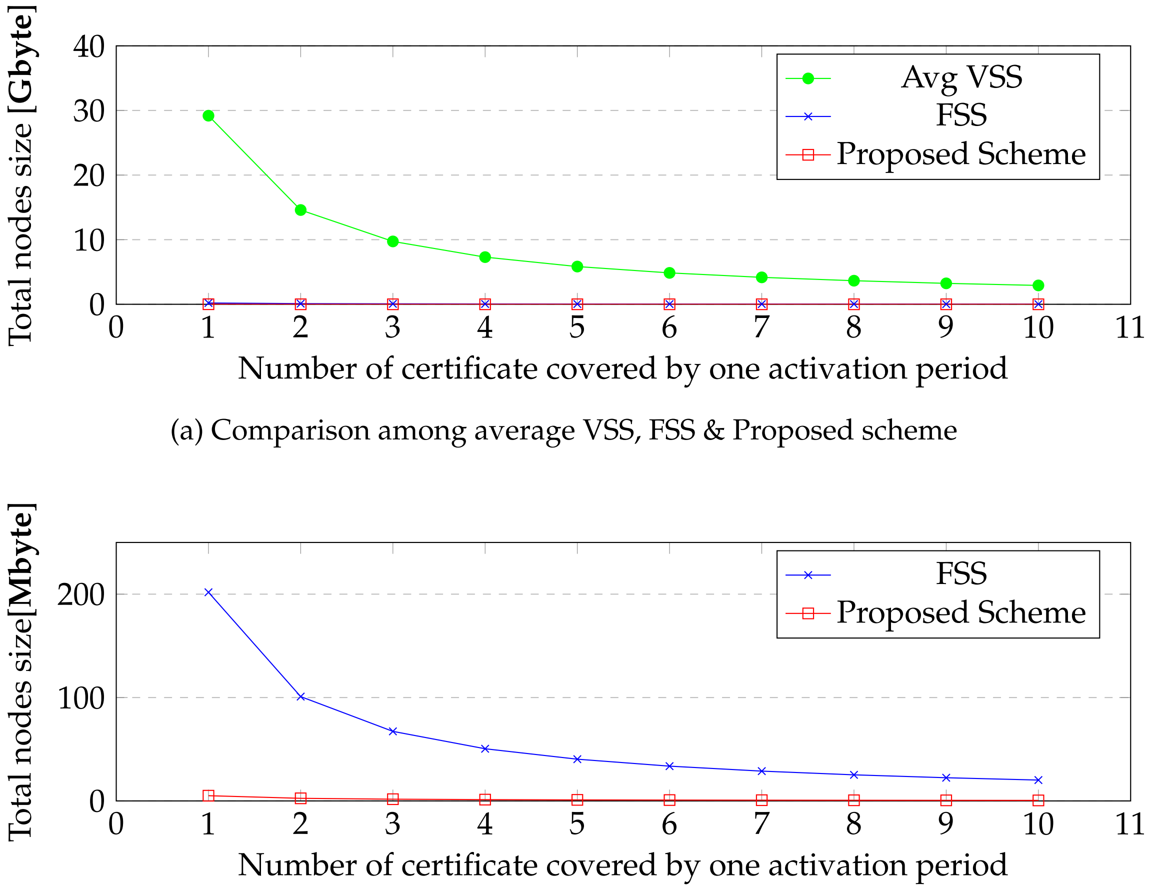
The number of nodes from ACPC that a vehicle must download varies depending on the number of revoked vehicles. Shortening the certificate validity and activation period together gives malicious vehicles less time to continue using the remaining certificates. Consequently, all vehicles have to download 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 nodes 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 get 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 50000 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 minutes only and the total valid period is 1.576.800 minutes (3 years), so to total certificates as well as $\tau$ is 315.576. The $i$ is the number of $t$ that is covered by one $a$, with a variation of $i$ we can see the graph in Figure 3.8 that our scheme compared to VSS and FSS, it uses the smallest total download of node size during three years usage. On average, as shown in Figure 3.8a, the average VSS required to download the most significant amount of data, and the most extensive data size reaches 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 3.8b. Our proposed scheme shows that the total data downloaded for various cover validity periods for each activation period is minimal. The most interesting 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.

### 3.3.7 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 3.3 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 done 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.



(a) Comparison among average VSS, FSS & Proposed scheme

(b) Comparison between FSS & Proposed scheme

Figure 3.8: The total amount of downloaded nodes by a vehicle in 3 years

Table 3.3: 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 |

# Chapter 4

# Modified Activation Code Delivery

## 4.1 Introduction

The application of V2X technology allows vehicles to communicate with other vehicles or roadside devices in real-time. They communicate wirelessly, generally based on DSRC and cellular technology (4G or 5G). Vehicles send messages to other vehicles about their position, direction, speed, and other relevant information so that each vehicle understands the situation of other vehicles around it. The message received by the vehicle must be ascertained for authenticity, lest someone sends a fake message for his benefit and interferes with the driving safety application. The standards organizations in Europe and the US use digital certificates to maintain message security of V2X. To manage digital certificates of the V2X, they use PKI with some adaptation mainly to meet four privacy key attributes: anonymity, pseudonymity, unlinkability, and unobservability [10]. In both standards car′s pseudonym certificates are used interchangeably over a short period. So that it is hard to trace the vehicle′s path using the pseudonym certificates.

The different pseudonym certificates over this short range cause some side effects. In addition to the increasingly complex structure of the PKI, the pseudonym certificate revocation becomes challenging to handle. Misbehaving vehicles must be removed from the V2X system to avoid damage and road accidents. For example, vehicles that spread inappropriate messages cause a wrong decision. The certificate authority must revoke such a vehicle′s certificate so that other vehicles are ignoring the messages spread by misbehaving vehicles.

Revoking the pseudonym certificate on a misbehaving vehicle is generally done using CRL. After the certificate authority gets information about the misbehaving vehicle, it identify the misbehaving vehicle. Then it inserts the certificate identity in the CRL to known by the end entities. However, there were many obstacles to delivering CRL to the vehicle timely, mainly due to the limited resources and dynamic network characteristics of V2X. One promising way to solve this certificate revocation problem is to apply the certificate activation techniques such as in ACPC[9] and IFAL[21].

Certificate activation is a technique in which encrypted certificates assigned to each period are given to the vehicle during registration. Then the vehicle needs a key/code of each period to decrypt/activate the certificate to use it. The certificate authority periodically sends the activation codes to the unrevoked vehicles, while not to revoked vehicles. As a result, the revoked vehicles can no longer use their certificates in the next period. This certificate activation technique has several advantages, including lower costs on network resources and the message verification process compared to standard CRLs.

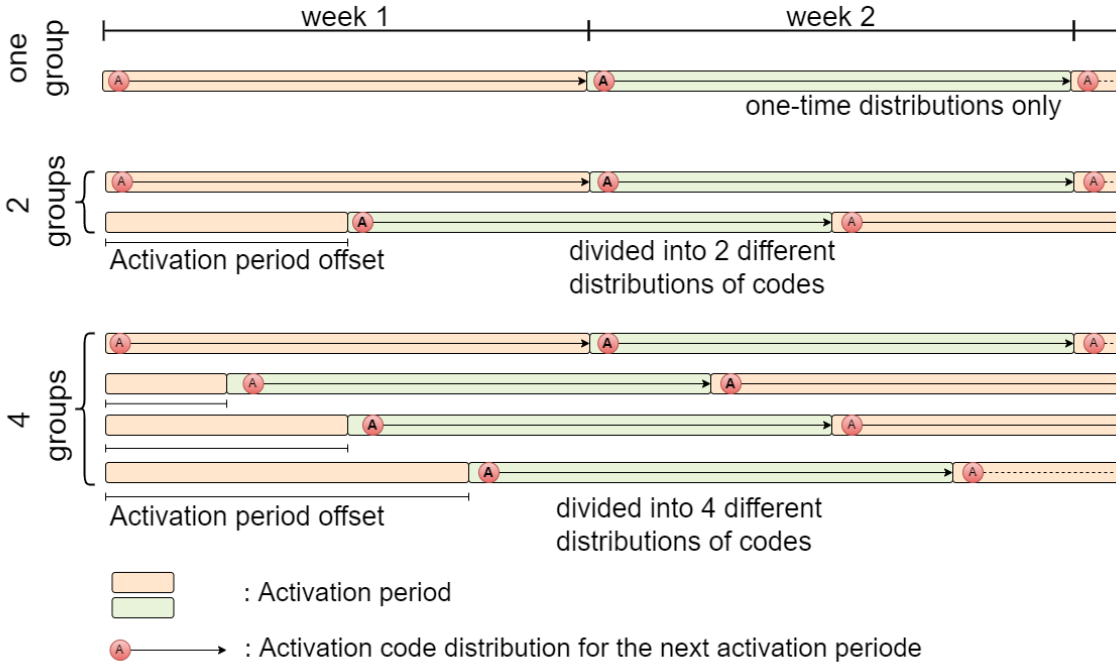
The certificate activation strategy still needs an improvement in the size of the activation codes when the number of revoked vehicles is small. That is, the size of the delivered activation codes is larger than the size of the CRL for a small number of revoked vehicles. Another problem is that all unrevoked vehicles must receive activation codes in the same period. It causes an additional network burden due to repeated broadcasts or simultaneous requests of the activation codes.

## 4.2 Contributions

We should fine out a new strategy for delivering activation certificates to solve the problems. This study evaluates the simultaneous delivery of activation codes for unrevoked vehicles in V2X communication. To reduce the size of sending activation codes, we divide the activation codes into several groups. Each group is sent at different periods to spare the network load. To do so, we introduce an activation period offset to facilitate the shift of the certificate activation period as shown in Fig. 4.1. Even if the entire vehicle has an activation code from the same tree root, vehicles have different certificate activation periods.

## 4.3 Related Work

The delivery technique of activation codes has not yet been discussed in previous studies. The IFAL does not use a binary tree, so the delivery of the activation codes depends on the policy file created at the beginning of registration. Suppose that the policy file is applied differently to the group of vehicles. The activation



one group
week 1
week 2
A
one-time distributions only
2 groups
Activation period offset
divided into 2 different distributions of codes
4 groups
Activation period offset
divided into 4 different distributions of codes
: Activation period
: Activation code distribution for the next activation periode

Figure 4.1: Activation code delivery with different activation period offset

codes can be sent at different times. However, the authors show a scenario of simultaneously broadcasting to all unrevoked vehicles, causing a gigabyte of delivery activation codes.

The ACPC has a better privacy protection than the IFAL. Like BCAM [7], ACPC broadcasts the activation codes to all unrevoked vehicles. However, it must send the activation codes simultaneously for all vehicles. Further research in uACPC has tried to exploit the ACPC property which allows the vehicle to fetch a sufficiently small activation codes via a unicast mechanism [12]. However, it also lacks in a mechanism to split the activation codes distribution at different times.

## 4.4 Preliminary results

According to the recommendation from SCMS, the validity of pseudonym certificates is one week. Suppose the activation codes are distributed within one week before the certificate starts to be used. In that case, the ACPC must broadcast the activation codes once a week to unrevoked vehicles. Meanwhile, our scheme can arrange two or more different distributions time within that period.

The provisional results show that dividing the activation codes at different times allows the activation codes broadcast size to be smaller than the original

ACPC. The original ACPC also sends all activation codes once a week. In Fig. 4.2, assume that total vehicle in the system is 1,048,576 unit, and number of unrevoked vehicle is 104,858 unit (10% of total vehicles) fixed to all period. If the ACPC activation codes are divided into two groups, the activation code's total size is half the original one because the delivery is done on two different days. That way, the network load at the delivery time is divided into two different times in the one-week activation period. Dividing an activation period into smaller parts can reduce the size of a broadcast activation codes.

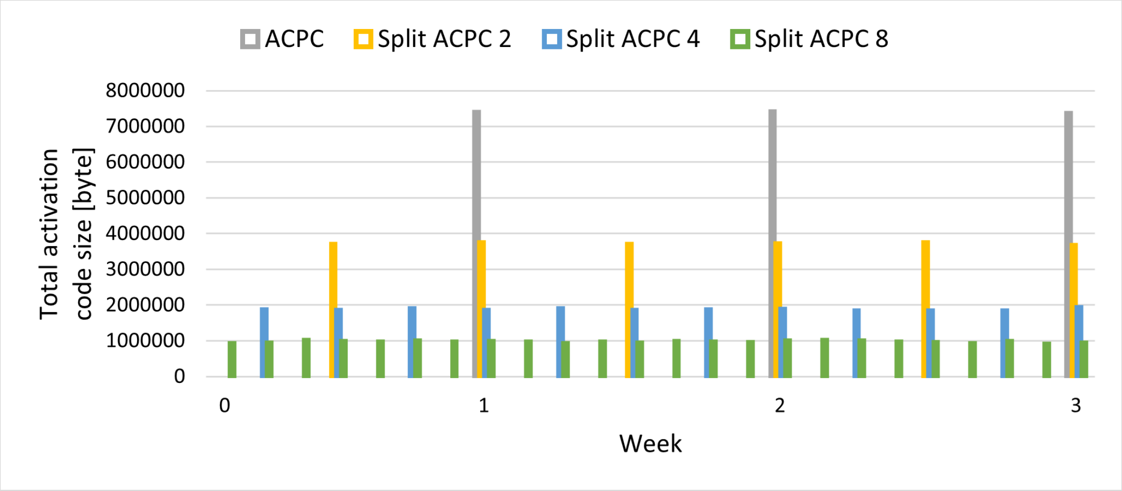


Figure 4.2: Activation code distribution size

# Chapter 5

# Conclusion

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 have information to 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 devices does not require encryption and authorization. The caching devices does not require any certificate authority control and does 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.

We also show that dividing the activation codes at different times allows the activation codes broadcast size to be smaller than the original ACPC

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

# Abbreviations

| | |
|---|---|
| ACPC | activation code for pseudonym certificate |
| BCAM | binary hash tree based certificate access management |
| BSM | basic safety message |
| C-ITS | cooperative intelligent transportation systems |
| C-V2X | cellular V2X |
| 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 | Europe |
| FSS | fixed-size subset |
| IEEE | Institute of Electrical and Electronics Engineers |
| IFAL | issue first activate later |
| ITS | intelligent transport system |
| LOP | location obscurer proxy |
| MA | Misbehavior Authority |
| NHTSA | National Highway Traffic Safety Administration |
| OBU | on-board unit |
| OEM | original equipment manufacturer |
| PCA | pseudonym certificate authority |
| PKI | public key infrastructure |
| RA | registration authority |
| RSU | road-side unit |
| SCMS | security credential management system |
| SMS | short message sevice |
| uACPC | activation code for pseudonym certificate |
| US | United States |

| | |
|---|---|
| USDOT | United States Department of Transportation |
| V2D | vehicle to device |
| V2I | vehicle to infrastructure |
| V2N | vehicle to network |
| V2P | vehicle to pedestrian |
| V2V | vehicle to vehicle |
| V2X | vehicle to everything |
| VPKI | vehicullar public key infrastructure |
| VSS | variable-size subset |
| WLAN | Wireless LAN |

# Bibliography

[1] J. Huang, D. Fang, Y. Qian, and R. Q. Hu, "Recent advances and challenges in security and privacy for v2x communications," *IEEE Open Journal of Vehicular Technology*, vol. 1, pp. 244–266, Jun. 2020. DOI: 10.1109/ojvt.2020.2999885.

[2] B. Brecht, D. Therriault, A. Weimerskirch, *et al.*, "A security credential management system for v2x communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, pp. 3850–3871, 12 Dec. 2018, ISSN: 15249050. DOI: 10.1109/TITS.2018.2797529. [Online]. Available: https://ieeexplore.ieee.org/document/8309336/.

[3] M. Hasan, S. Mohan, T. Shimizu, and H. Lu, "Securing vehicle-to-everything (v2x) communication platforms," *IEEE Transactions on Intelligent Vehicles*, vol. 5, no. 4, pp. 693–713, 2020. DOI: 10.1109/TIV.2020.2987430.

[4] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, and S. Manickam, "Survey of Authentication and Privacy Schemes in Vehicular ad hoc Networks," *IEEE Sensors Journal*, vol. 21, no. 2, pp. 2422–2433, 2021, ISSN: 15581748. DOI: 10.1109/JSEN.2020.3021731.

[5] M. Raya, D. Jungels, P. Papadimitratos, I. Aad, and J.-P. Hubaux, "Certificate revocation in vehicular networks," *Laboratory for computer Communications and Applications (LCA) School of Computer and Communication Sciences, EPFL, Switzerland*, pp. 1–10, 2006.

[6] ETSI, "Intelligent transport systems (its); security; its communications security architecture and security management," European Telecommunications Standards Institute, Tech. Rep. TS 102 940, V1.3.1, 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.03.01_60/ts_102940v010301p.pdf.

[7] V. Kumar, J. Petit, and W. Whyte, "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*, ser. WiSec '17,

Association for Computing Machinery, 2017, pp. 145–155, ISBN: 9781450350846. DOI: 10.1145/3098243.3098257. [Online]. Available: https://doi.org/10.1145/3098243.3098257.

[8] E. R. Verheul, "Activate later certificates for v2x–combining its efficiency with privacy," *Cryptology ePrint Archive*, 2016.

[9] M. A. Simplicio, E. L. Cominetti, H. K. Patil, J. E. Ricardini, and M. V. M. Silva, "Acpc: Efficient revocation of pseudonym certificates using activation codes," *Ad Hoc Networks*, vol. 90, p. 101 708, Jul. 2019, ISSN: 15708705. DOI: 10.1016/j.adhoc.2018.07.007. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1570870518304761.

[10] ETSI, "Intelligent transport systems (its); security; trust and privacy management; release 2," European Telecommunications Standards Institute, Tech. Rep. TS 102 941 - V2.1.1, 2021. [Online]. Available: https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx.

[11] M. A. Simplicio, E. L. Cominetti, H. K. Patil, J. E. Ricardini, and M. V. M. Silva, "Revocation in vehicular public key infrastructures: Balancing privacy and efficiency," *Vehicular Communications*, vol. 28, p. 100 309, Apr. 2020, ISSN: 22142096. DOI: 10.1016/j.vehcom.2020.100309.

[12] H. Cunha, T. Luther, J. Ricardini, H. Ogawa, M. Simplicio, and H. K. Patil, "Uacpc: Client-initiated privacy-preserving activation codes for pseudonym certificates model," *SAE International Journal of Transportation Cybersecurity and Privacy*, vol. 3, no. 11-03-01-0004, pp. 57–77, 2020.

[13] IEEE, "Ieee standard for wireless access in vehicular environments (wave) - networking services," Tech. Rep. IEEE Std 1609.3-2010, 2010, pp. 1–144. DOI: 10.1109/IEEESTD.2010.5680697.

[14] X. Lin, J. G. Andrews, A. Ghosh, and R. Ratasuk, "An overview of 3gpp device-to-device proximity services," *IEEE Communications Magazine*, vol. 52, no. 4, pp. 40–48, 2014. DOI: 10.1109/MCOM.2014.6807945.

[15] Q. Wang, D. Gao, and D. Chen, "Certificate revocation schemes in vehicular networks: A survey," *IEEE Access*, vol. 8, pp. 26 223–26 234, 2020. DOI: 10.1109/ACCESS.2020.2970460.

[16] M. D. Furtado, R. D. Mushrall, and H. Liu, "Threat analysis of the security credential management system for vehicular communications," in *2018 IEEE International Symposium on Technologies for Homeland Security (HST)*, IEEE, 2018, pp. 1–5.

[17] B. Fernandes, J. Rufino, M. Alam, and J. Ferreira, "Implementation and Analysis of IEEE and ETSI Security Standards for Vehicular Communications," *Mobile Networks and Applications*, vol. 23, no. 3, pp. 469–478, 2018, ISSN: 15728153. DOI: 10.1007/s11036-018-1019-x. [Online]. Available: https://doi.org/10.1007/s11036-018-1019-x.

[18] A. Ghosal and M. Conti, "Security issues and challenges in V2X: A Survey," *Computer Networks*, vol. 169, p. 107 093, 2020, ISSN: 1389-1286. DOI: 10.1016/J.COMNET.2019.107093.

[19] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "Misbehavior detection and efficient revocation within vanet," *Journal of Information Security and Applications*, vol. 46, pp. 193–209, Jun. 2019, ISSN: 22142126. DOI: 10.1016/j.jisa.2019.03.001.

[20] CAMP, *Security credential management system proof-of-concept implementation ee requirements and specifications supporting scms software release 1.2.2*, https://www.its.dot.gov/research_areas/cybersecurity/scms/SCMS-CV-Pilots-Documentation_26838136.html, Accessed: 02-02-2022, 2018.

[21] E. Verheul, C. Hicks, and F. D. Garcia, "Ifal: Issue first activate later certificates for v2x," in *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, IEEE, 2019, pp. 279–293.

[22] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, "A security credential management system for v2v communications," in *2013 IEEE Vehicular Networking Conference*, 2013, pp. 1–8. DOI: 10.1109/VNC.2013.6737583.

[23] W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," in *Annual International Cryptology Conference*, Springer, 1998, pp. 137–152.