5GAA Efficient Security Provisioning System

5GAA Automotive Association
White Paper

CONTACT INFORMATION:

Lead Coordinator – Thomas Linget
Email: thomas.linget@5gaa.org

MAILING ADDRESS:

5GAA c/o MCI Munich
Neumarkter Str. 21
81673 München, Germany
www.5gaa.org

VERSION:	1.0
DATE OF PUBLICATION:	18.05.2020
DOCUMENT TYPE:	White Paper
CONFIDENTIALITY CLASS:	P (Public use)
REFERENCE 5GAA WORKING GROUP:	Working Group 7
DATE OF APPROVAL BY 5GAA BOARD:	19.02.2020

Contents

1. **Abbreviations** 4
2. **Introduction** 6
   - 2.1 **Motivation** 6
   - 2.2 **Areas of Potential Simplification** 7
     - 2.2.1 Bootstrapping/Enrolment 8
     - 2.2.2 Network and System Architecture 8
     - 2.2.3 Certificate Provisioning and Management 8
     - 2.2.4 Trust Anchor Management 9
   - 2.3 **Other Considerations** 9
     - 2.3.1 Distribution of Trust Lists and Revocation Lists 9
3. **Proposed Simplifications** 10
   - 3.1 **Simplifications of the Bootstrapping Enrolment Process** 10
     - 3.1.1 Key Injection 10
     - 3.1.2 Bootstrapping as a Service 10
   - 3.2 **Simplifications to Organisational Separation of Duties** 12
     - 3.2.1 Linkage Authority Simplifications 12
     - 3.2.2 Removing Location Obscurer Proxy 13
     - 3.2.3 Removing the Registration Authority Shuffling 13
   - 3.3 **Simplifications of the Certificate Provisioning and Management** 13
     - 3.3.1 More Efficient Provisioning Protocols 13
     - 3.3.2 Pre-provisioning of Certificates 15
     - 3.3.3 Efficient Revocation 15
   - 3.4 **Simplification of Trust Anchor Management** 16
     - 3.4.1 Existing Single Authority Trust Anchor Management 16
     - 3.4.2 Elector-based Trust Anchor Management Scheme 17
     - 3.4.3 Proposed Scheme for ESPS 17
4. **Other Considerations** 19
   - 4.1 **Distribution of CTLs and CRLs** 19
5. **Conclusions** 20
6. **References** 21

1. Abbreviations

For the purpose of the present document, the following abbreviations apply:

5GAA	5G Automotive Association
ADAS	Advanced Driver Assistance Systems
APN	Access Point Name
CA	Certificate Authority
CAV	Connected and Autonomous Vehicles
CCMS	C-ITS Security Credential Management System
C-ITS	Cooperative Intelligent Transport Services
CPA	Certificate Policy Authority
CPOC	Central Point of Contact
CRL	Certificate Revocation List
CSR	Certificate Signing Request
C-V2X	Cellular Vehicle-to-Everything
DCM	Device Configuration Manager
ECA	Enrolment Certificate Authority
ECDSA	Elliptic Curve Digital Signature Algorithm
ECTL	European Certificate Trust List
EE	End Entity
eSIM	Embedded SIM
ESPS	Efficient Security Credential Provisioning System
ETSI	European Telecommunications Standards Institute
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
GCCF	Global Certificate Chain File
HSM	Hardware Security Module
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
ITS	Intelligent Transport Services
LA	Linkage Authority
LOP	Location Obscurer Proxy
MA	Misbehaviour Authority
MitM	Meddler-in-the-Middle

MNO	Mobile Network Operator
NIST	National Institute of Standards and Technology
OBU	Onboard Unit
OEM	Original Equipment Manufacturer
PKI	Public Key Infrastructure
QR	Quantum Resistant
RA	Registration Authority
RCA	Root Certificate Authority
RSU	Roadside Unit
SE	Secure Enclave
SCMS	Security Credential Management System
SIM	Subscriber Identity Module
TLM	Trust List Manager
TLS	Transport Layer Security
UE	User Equipment
USIM	Universal Subscriber Identity Module
V2I	Vehicle-to-Infrastructure
V2N	Vehicle-to-Network
V2P	Vehicle-to-Pedestrian
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything

2. Introduction

Vehicle-to-everything (V2X) communication is at our doorsteps. It is a key part of the future of connected vehicles and autonomous driving as it enables infrastructure, pedestrians and vehicles to interact, thus taking the transportation ecosystem to the next level. Security plays an important role in building trust in V2X, protecting users' privacy, and enabling safety, efficiency .and comfort.

Efforts to reinforce trust in this ecosystem are driving global initiatives to develop, standardise and implement Security Credential Management Systems (SCMS). As a consequence, different stakeholders have put forward their requirements leading to differing, non-interoperable regional designs. The 5G Automotive Association (5GAA) has evaluated existing system designs and their regulatory requirements, as well as identified some new 'advanced' features. The resulting recommendations for improved design fulfilling these security and privacy requirements in a large-scale system are outlined in this paper.

2.1 Motivation

The 5G Automotive Association is a global, cross-industry organisation of companies from the automotive, information, communication and technology industries. With the objective to integrate new technical opportunities in the automotive world, as afforded by widespread cellular connectivity, and to identify potential design simplifications, an analysis and evaluation of existing system designs has been completed over the last year. These existing designs are region-specific (USA [], [] and Europe []) and not fully interoperable due to differing security and privacy requirements.
Some ecosystem stakeholders within 5GAA challenged this status quo on several levels and evaluated these regional V2X security approaches. The goals of this effort were as follows:

- Update assumptions given the current technology landscape
- Improve on previous designs to take advantage of cellular connectivity
- Harmonise technologies across regions where possible
- Identify potential design simplifications to increase efficiency
- Identify avenues to decrease development and operational costs, and
- Support upcoming production-level deployments on a global scale.

The resulting optimised system is designed to balance the security and privacy principles of existing systems with the above-mentioned goals. The rest of this paper summarises these design simplifications, discusses their rationale and impact, and proposes an updated design for large-scale deployment and cross-regional interoperability called the 'Efficient Security Provisioning System' (ESPS).

2.2 Areas of Potential Simplification

The following sections outline potential simplifications to the existing V2X credential management systems. As an example, Figure 1 shows a diagram of the system components for the US Security Credential Management System (SCMS) of [1], [2], [4]. Architectures of the EU C-ITS Security Credential Management System (CCMS) are given in, e.g., [3] or [5].

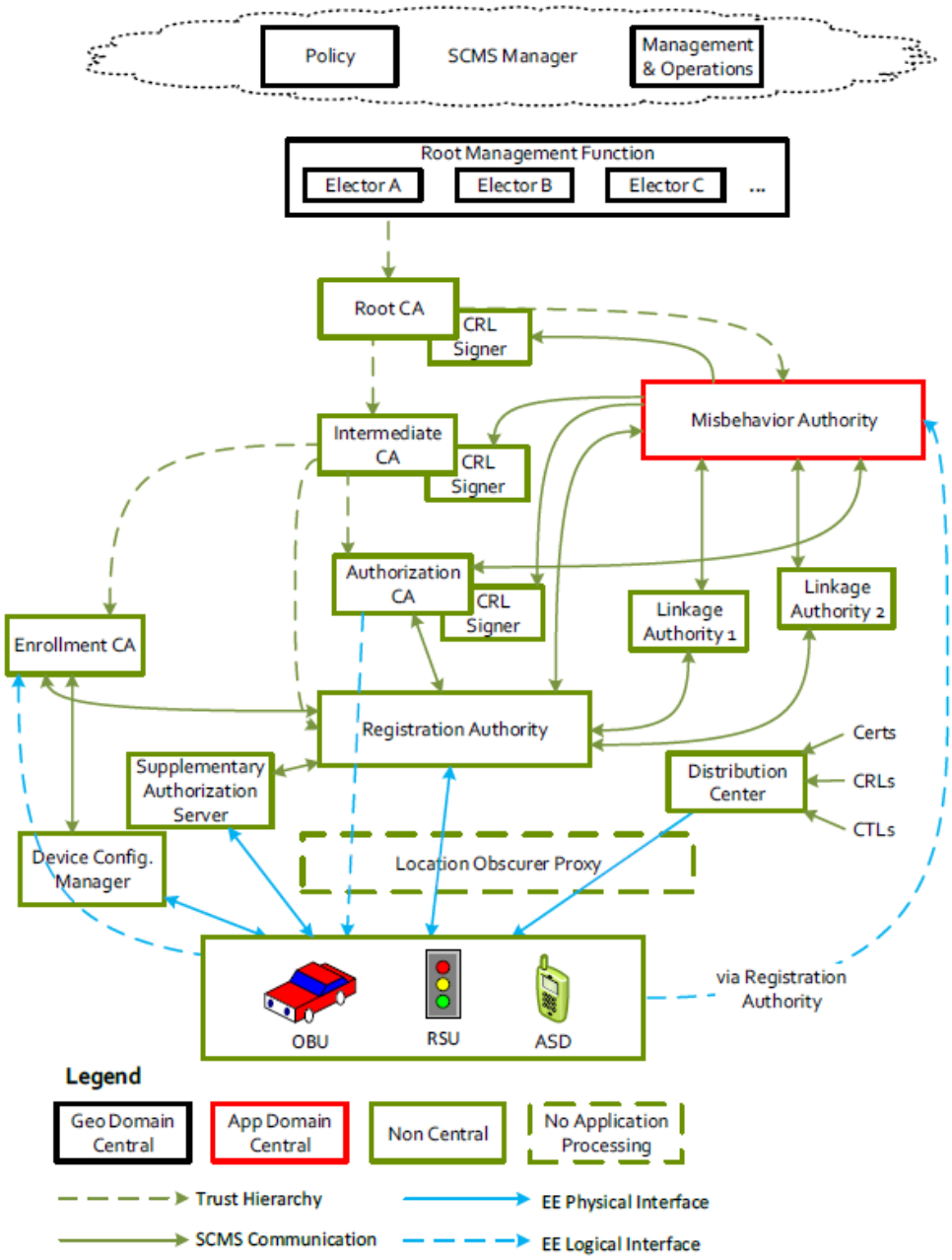

Figure 1: The US Security Credential Management System

2.2.1 Bootstrapping/Enrolment

In any SCMS, **bootstrapping** is the process that gets participating devices – e.g. vehicle Onboard Unit (OBU), Roadside Unit (RSU), also called End Entities (EEs) from a Public Key Infrastructure (PKI) perspective – into a state in which they can operate in the V2X ecosystem. This process includes obtaining and then storing security-critical information in a hardware component called a Secure Enclave (SE). Due to security – and in some regions, regulatory – requirements, private keys corresponding to both enrolment certificates and authorisation certificates (which include pseudonym, application, identification certificates or authorisation tickets) must be stored and used exclusively within an SE after bootstrapping [3] [6].

Furthermore, in some regions policy demands that all key pairs are generated inside the SE instead of being placed into the SE from outside (e.g. being injected) [3]. Generating a key pair and obtaining a respective certificate from an Enrolment Certificate Authority (ECA) may take valuable time or require a secure environment, which may be difficult to instantiate in existing production processes. This paper describes in section 3.1 alternative options to streamline that process in a secure manner by utilising the cellular/mobile infrastructure.

2.2.2 Network and System Architecture

A PKI system contains several components, including hierarchical Certificate Authorities, Registration Authorities, Revocation/Trust List Distribution Centres, and the like. For the V2X communication credential management, some entities were added to the system architecture to support privacy requirements, protecting vehicles from outside as well as inside attacks.

The SCMS was designed so that "no single entity" within the Management System can relate a pseudonym certificate to a vehicle or two pseudonym certificates to the same vehicle, which would enable long-term driver tracking. Several of the elements of the SCMS support this goal by virtue of the **organisational separation principle**: the Location Obscurer Proxy, the separate Registration Authority between the EE and the Application/Pseudonym CA, the twin Linkage Authorities, the shuffling of certificate requests at the RA, and other security measures.

The organisational separation principle is updated in section 3.2 in keeping with the evolution of communication technology, resulting in simplifications of the system architecture.

2.2.3 Certificate Provisioning and Management

Certificate Provisioning and **Management of Certificates** throughout their lifecycle is a key aspect of any PKI, but poses stringent requirements on a V2X PKI because of the sheer number of certificates to issue at each EE. The large number of certificates is to limit reuse and thus vehicle tracking, achieving privacy of location over time [7], [8].

Since the publication of the designs for SCMS [1] and CCMS [3], new and more efficient protocols for certificate provisioning have been proposed. This paper discusses in section 3.3 several ways to make certificate provisioning and management more efficient while maintaining the security needed to provide system integrity.

2.2.4 Trust Anchor Management

Trust anchor components (i.e. typically Root Certificate Authorities (RCA), but in the case of SCMS [1] Electors and in case of the CCMS [3] the TLM – entities that are inherently trusted) play a vital role in any credential management system, since the security of all EE authentication and communication relies on the trust anchor. This paper describes how specific features of the trust anchor components can be redistributed and/or merged, to achieve a simplification of the credential management architecture itself.

In this vein, two different trust anchor management schemes (elector-based, or single authority with a central trust list) are described, and a **harmonised trust anchor management scheme** is also described. This new scheme aims not only for simplification but also for robustness, resilience, flexibility, and interoperability across jurisdictions regarding deployment and administration.

2.3 Other Considerations

2.3.1 Distribution of Trust Lists and Revocation Lists

Lastly, this paper addresses some of the aspects of a V2X PKI system that are either not well described or not harmonised in current systems: namely, the options for distribution of trust lists and certificate revocation lists from the network to the vehicles.

3. Proposed Simplifications

This section describes the aforementioned simplifications for the ESPS in more detail. These simplifications suggest themselves in view of the cellular connection capabilities of today's V2X devices, as well as from a change in the policy trends of other industry verticals, which shift the onus of protecting the consumers' privacy from a mainly technical solution to a mainly procedural one at the (PKI) operator.

3.1 Simplifications of the Bootstrapping Enrolment Process

The first step of preparing a device for V2X communication operation is 'bootstrapping'. It aims to provide to the EE all necessary key pairs and Certificate Authority (CA) information including their certificates. All security-critical information is stored in EE's SE. Bootstrapping can be performed at the production line or in the field. If a safety mandate is in place, it is assumed that the V2X system of a vehicle has to be fully provisioned and operational before the vehicle is driven on a public road. Otherwise, bootstrapping at a dealership is a reasonable option, especially since the bootstrapping process takes valuable time on the fast-paced production line of the carmaker or the supplier of the V2X system.

The key requirements in this process are that only trusted EEs, which can mean 'certified' in some jurisdictions, get bootstrapped and only authentic keys and information are provisioned to an EE.

3.1.1 Key Injection

Keys can be generated inside of the EE's SE or generated outside of the EE in a secure environment, and then introduced into the EE's SE. Generating the key pair inside the SE may take up valuable time and increase complexity on the production line. If the key pair is generated elsewhere and then 'injected' into the SE, this has some advantages when carried out securely. The following variants for key generation (subject to best practices such as NIST [15]) can be identified:

1. Key generation inside a secure enclave: the enrolment certificate key pair is generated in the SE of the End Entity during production, and enrolment is performed in a secure environment; **or**
2. Key injection before enrolment: the certificate key pair is generated in a SE outside the EE and is injected into the EE's SE in a secure environment before enrolment leaving the exchange to take place between the ECA and the EE, just as if the key pair had been generated inside the EE's SE; **or**
3. Key injection of all credentials: the key generation, the enrolment exchange, and potentially, the pseudonym certificate request exchange is done by a SE outside the EE, and then all keys and certificates are securely injected into the EE's SE, but not necessarily in a secure environment.

3.1.2 Bootstrapping as a Service

In this section, we describe ways in which aspects of the bootstrapping process could be provided as a service to the OEM, particularly by the Mobile Network Operator (MNO).

The device identity and security management used in current cellular/mobile networks can be leveraged by third-party applications and servers.

3GPP has standardised a mechanism for application-layer security associations to be established, bootstrapped from the pre-existing mobile network authentication capability. This is called the Generic Bootstrapping Architecture (GBA) [7]. It is part of a wider set of specifications called Generic Authentication Architecture (GAA). Based on the secure authentication and key agreement between Universal Subscriber Identity Module (USIM) and MNO, it establishes a shared key between the EE and an application 'V2X server' (generally not owned by the MNO, but interfacing to a node run by the MNO). This shared key would typically be used for a secure TLS tunnel between EE and application server, although other uses are also possible.

In this instantiation, the USIM with its in-built keys is the only cryptographic component needed to establish a secure and trustworthy connection to the ECA under the assumption that the connection between the USIM and the EE's SE is secure and mutual authentication as legitimate devices is given. The unique key shared between USIM and MNO is used to set up a secure tunnel – typically TLS – between the EE and the ECA, shown as 'V2X server'. The EE needs to know the address of the ECA as there is no automatic routing. An important point is that GBA does not need a cellular connection – it works equally well over WiFi or a wired connection. It does require the presence of a USIM. Notably, this scheme relies on the assumption that the manufacturer is provided with dedicated USIMs and that the manufacturer and the supply chain can be trusted to put only those dedicated USIMs in genuine EEs.

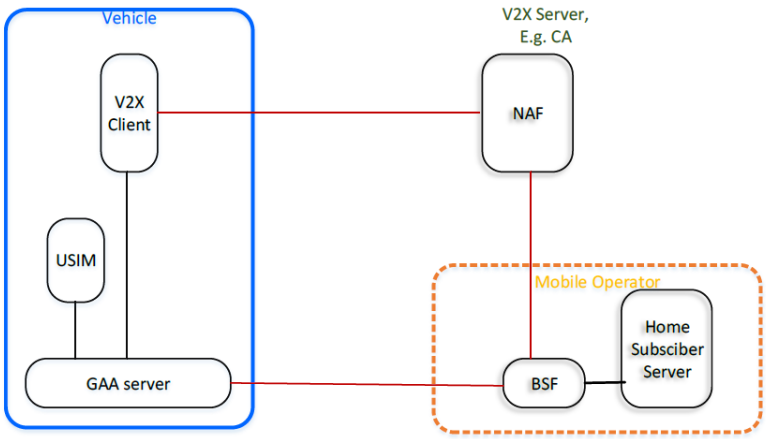

Figure 2: Generic Bootstrapping Architecture

Figure 2 illustrates GBA and the components required for this solution are:

- A software component in the device – the GAA Server – that provides generic GBA support
- Software in the device's V2X client that interfaces to that GAA server software
- A USIM communicating to the GAA server software
- Software in the ECA called a Network Application Function (NAF)
- A dedicated new mobile network component called the Bootstrapping Server Function (BSF)

In this solution, there is no need for the EE to have the ECA's X.509 certificate available in advance. This proposal only works for USIM-equipped EE and requires that an internet connection is established before enrolment can take place. If these requirements are acceptable, it allows the vehicle to self-enrol. Furthermore, one crucial point in the embedded USIM's lifecycle is the provisioning of the MNO profile. When setting up the OBU, provisioning of a profile could potentially be done in a secure environment. Once the OBU is in the field, the MNO profiles need to be provisioned remotely onto the embedded USIM. However, processes and technical capabilities for MNO profile provisioning have not been investigated thoroughly enough to have a profound understanding of the security related aspects, in order to derive any recommendation for vehicle bootstrapping.

In conclusion, in the ESPS, key injection is supported and, given further research and proof of a secure end-to-end architecture, MNO-assisted bootstrapping will be supported depending on threat models, local regulation, or business considerations.

3.2 Simplifications to Organisational Separation of Duties

The issue of privacy protection against insider attacks – whereby some network functions collude to gather data for tracking of vehicles – was paramount in the design of the US SCMS, and to some extent the EU CCMS. This led to the criterion of "no single entity" [should be able to track a vehicle], implemented by techniques including organisational separation of duties. This principle resulted in credential management functionality being split amongst various system components, and expected to be operated by separate entities.

With the evolution towards cellular-V2X communications, the MNO joins the ecosystem. For Cellular-V2X to work properly, the OBU needs to connect to the mobile network frequently, and so as a result of this process, the MNO acquires location information. Therefore, we re-evaluated the results of the risk assessment. To start with, we note that mobile network operators are already established as trusted parties, operating under regulatory constraints, given their access to location-sensitive information. With that, the level of privacy protection within the MNO becomes the required threshold for location privacy protection within the overall V2X system, whether or not the MNO is actually participating in a given V2X communication. As a result, the protection of privacy-sensitive information should shift from a technical and organisational solution to an SCMS operator-specific solution, since MNOs are trusted parties based on MNO specific solutions. This allows simplifications of the SCMS and CCMS design.

Our evaluation is supported by an analysis of the FMVSS-150 NPRM in [8] and supplemental material to the NPRM [9]. The supplemental material to the FMVSS-150 NPRM addresses organisational separation, pointing out that there is no need to have multiple, independent organisations running parts of the SCMS for the sake of privacy. Furthermore, the SCMS Manager ultimately decides on the rules/policy governing separation. Note in this document that the SCMS Manager is assumed to be an industry-wide coalition of stakeholders in the US market.

With organisational separation clarified in the context of a modern V2X communication system and network, several simplifications to the system present themselves. They involve the merging or removal of some components and/or features.

It is worth noting that removing the "no single entity" criterion could reintroduce the risk of vehicle tracking by some entities such as the combined RA/LAs. However, this overall increase in vehicle tracking risk is similar to the existing mobile coverage risk; the MNO has operational knowledge of the current radio network connection and location of subscribed devices even while in idle mode.

3.2.1 Linkage Authority Simplifications

The LAs in SCMS provide linkage values embedded in pseudonym certificates to enable efficient and privacy-preserving revocation. If there were a single LA, it could link pseudonym certificates as belonging to one EE, hence the original design employs two LAs that split the task of providing linkage values in a way that no individual LA is able to link pseudonym certificates as belonging to the same EE.

way that no individual LA is able to link pseudonym certificates as belonging to the same EE.

A simplification is to merge the two Linkage Authorities and integrate them into the Registration Authority in the ESPS. This would result in a single LA with two linkage seeds integrated organisationally with the RA, accompanied by organisational and operational means within the RA/LA to protect against linking of pseudonym certificates via linkage values.

The benefit of this approach is that it reduces the organisational effort to operate two separate LAs, hence reducing the overall effort of operating the SCMS. This approach is effective if organisational security within the LA is clearly and convincingly demonstrated.

3.2.2 Removing Location Obscurer Proxy

The Location Obscurer Proxy (LOP) in the SCMS is located between the EE and RA. It removes data about the vehicle, such as the IP address (and thus the approximate physical location), so that the RA does not know where the EE is located when it establishes a connection to it.

A further simplification would be to remove the LOP from the ESPS design because some of its functions are already covered by other network components, such as load balancers. The EE's IP address would also only reveal a rough location of the EE and only when the EE is connecting to the RA. What's more, emerging technological advancements like the IPv6 privacy extension and TLS 1.3 enhance privacy capabilities and reduce the exposed data in transport.

3.2.3 Removing the Registration Authority Shuffling

Another simplification in the ESPS is to remove the RA Shuffling of EE requests for certificates. In the SCMS design, the RA creates a set of requests to issue pseudonym certificates via the butterfly key expansion mechanism and shuffles requests for different EEs before sending them to the Authorisation CA (ACA). With this, the ACA is unable to link individual requests to the same EE based on their order.

With the removal of the "no single entity" criterion, as explained above, the shuffling in the RA could be removed altogether, or made optional. If shuffling is not performed and the pseudonym certificate requests are sent as they come in, then the ACA needs to ensure organisational security, to avoid the risk that an 'ACA insider' links issued pseudonym certificates to a given EE.

Removing or reducing RA Shuffling would lower computational effort in the RA but increase organisational security effort in the ACA. This lowers the direct benefit, however overall SCMS computing costs are comparatively small, so removing RA Shuffling may still be worth the effort.

3.3 Simplifications of the Certificate Provisioning and Management

3.3.1 More Efficient Provisioning Protocols

One of the main goals of the SCMS, as well as the CCMS, is to enable the construction of a secure and privacy-preserving V2X ecosystem [1] [3]. To accomplish this task, the SCMS provisions EEs with an

arbitrarily large batch of pseudonym certificates, using an efficient process called butterfly key expansion. This is in contrast to the CCMS, where each certificate requires an individual certificate signing request (CSR) [10].

The butterfly key expansion protocol ensures that only the EE knows the private key allowing signatures to be generated with the received pseudonym certificates, while at the same time neither the ACA nor RA can link different pseudonym certificates together or identify the owner. Given their respective policies, the ACA and RA would only be allowed to reverse this privacy protection in the event of identified misbehaviour. EEs can then protect their privacy by frequently changing the respective pseudonym certificates, thus avoiding tracking and ensuring privacy by design.

One source of inefficiency in the original butterfly key expansion protocol [1] is that an EE must send two public keys and two expansion functions to the RAs. A simpler and more efficient version of the butterfly key expansion process was proposed in [11]. This new design, called the Unified Butterfly Key (UBK) expansion, improves the original key expansion process by coupling the encryption and signature keys in a verifiable manner, therefore requiring an EE to send only one public key and only one expansion function. The UBK process is summarised in Figure 3. The numbers in circles indicate the sequence of steps involved in this process and they are detailed afterwards.

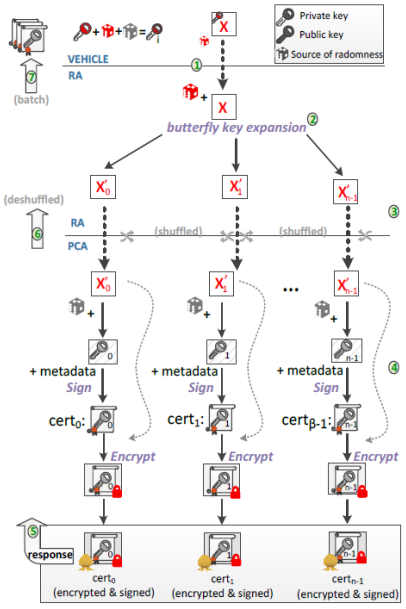

Figure 3: Unified Butterfly Key Expansion

The following list describes the UBK protocol:

1. Each EE generates a single caterpillar public/private key pair and sends the public counterpart X together with one expansion function to the RA.
2. The RA proceeds by generating multiple cocoon public keys X' from this caterpillar public key using the expansion function and, as before, shuffles cocoon keys from different EEs.
3. The RA sends individual pseudonym certificate requests to the PCA, each one containing one single cocoon key X'.
4. The PCA randomises the received cocoon public key to obtain the EE's butterfly public key, creates and signs one pseudonym certificate for this butterfly key, and encrypts that certificate and the random value used to generate the butterfly public key with the originally received (i.e., non-randomised) cocoon public key X'. The PCA then signs the encrypted package.
5. The encrypted package is sent back to the respective RA.

6. The encrypted package is sent back to the respective RA.
7. Finally, the EE can verify the signature of the encrypted package, decrypt the received certificate and random value, verify that the certificate is correctly signed by the PCA, and recover the corresponding butterfly private key.

Pseudonym certificates generated in this manner remain unlinkable to each other or to the EE (except in the event the EE was found to be misbehaving), as with the original butterfly key expansion.

It is important that all entities in the system are aware of whether the original butterfly key expansion protocol or UBK is being used by any given RA.

In summary, according to [11], the benefits of the UBK optimisation, under certain load conditions, are as follows:

- It reduces by half the number of keys sent from the EE to the RA, as well as from the RA to the PCA (two keys are replaced by a single key).
- It reduces by half the number of expansion functions sent from the EE to the RA.
- It reduces by half the number of expansions executed by the RA.
-

3.3.2 Pre-provisioning of Certificates

Temporary, short-lived pseudonym certificates are (pre)provisioned into an EE periodically, so that it always has a sufficient number to cycle through as it engages in V2X communication. Based on an updated connectivity model, which assumes more frequent connectivity between EEs and the PKI and the guidance given in [3], decreasing the time between issuance and expiry of pre-provisioned pseudonym certificates to a maximum of three months is recommended. This is in order to balance the usefulness of the service – an EE without valid certificates cannot send V2X messages and there might be circumstances where an EE is not able to connect to the PKI for some time – with the timely removal of an EE from the system in the event an attacker is able to gain access to the EE's private keys.

The CCMS already implements this guidance [3], due to the lack of an efficient revocation mechanism. Therefore, in the CCMS, an attacker that is able to gain access to an EE's private keys would have a period of up to three months until running out of pre-provisioned certificates, in the event that the EE was immediately detected and prevented from getting any new certificates. This circumstance leads to the recommendation in the next section.

3.3.3 Efficient Revocation

End Entities use their V2X certificates to sign V2X messages, and so the impact of a malicious actor, though geographically limited, can potentially affect the integrity of V2X communication and consequently the actions of other traffic participants. An efficient revocation of pseudonym certificates has been deployed before by the use of linkage values [14] [2], which enable the revocation of all of an EE's authorisation certificates with a single CRL entry. Furthermore, the use of cellular connectivity allows frequent updates of CRLs.

Additionally, the certificate authorities (Root, Intermediate, and Authorisation) hold certificate-signing certificates, and due to their importance in the trust chain employed in vehicle certificates, their timely revocation must be supported.

We recommend for the ESPS to implement blacklisting of enrolment certificates to block misbehaving EEs from getting additional certificates, and revocation through linkage values on certificate revocation lists (CRLs) for authorisation certificates. The reason is that there can be circumstances where immediate revocation is required to mitigate the occurrence of false positives and a negative public perception of V2X. This would also prepare the system for a later deployment of a Misbehaviour Authority, which might not be deployed on 'Day 1'.

3.4 Simplification of Trust Anchor Management

As discussed in [1], trust anchor management is an important part of any PKI, but especially in a V2X PKI, not only during normal operation but especially during disaster recovery (e.g. compromise, discontinuation of service due to natural or man-made disaster). The challenge is to build resilience against disaster on any level of the PKI hierarchy while at the same time keeping the ability to send, receive and validate V2X messages at the device level without requiring physical access to devices during recovery operations. Two scenarios present themselves:

- If there is no resilience against disaster there will be system outages that will impact the performance of V2X safety applications, with customers potentially having to be informed, which leads to increased costs.
- Requiring physical access to a device during recovery operations would entail at least a voluntary EE recall, which again would incur costs.

This leads to the following propositions for the ESPS:

- The V2X PKI manager should have a way to manage trust anchors and a disaster recovery plan to allow for timely mitigation, while reducing recovery costs and time; the V2X PKI manager should implement an established certificate and security policy for trust anchor management and a standardised way to change trust anchor certificates.
- Trust anchor management should be automated as much as possible, and the trust anchor credentials should roll over on a regular basis, in order to practice for recovery when a disaster actually strikes. The recovery procedure should also avoid the need to have physical access to EEs.

The main reason for these proposed measures is that the system can automatically and regularly rollover, and in the event of a disaster, the same process can be followed for revocation and replacement. This increases the chances of timely disaster recovery and minimises the impact of system outages.

Although there is some additional operational cost involved in an Elector-based Trust Anchor Management, as described in [1], compared to a system with a single authority (TLM) signing a central trust list, as specified in [5], [3], the advantages in terms of system robustness and resilience outweigh the costs. Such a trust anchor management system is deemed to be more resilient to disasters and an important feature for any V2X PKI. In the following, we describe the existing approaches and the proposed approach.

3.4.1 Existing Single Authority Trust Anchor Management

A single TLM is endorsed by a policy authority, and this TLM outputs a regional Certificate Trusted List

(e.g. European Certificate Trust List - ECTL) containing the set of trusted RCAs. The CTL is distributed as designed in the CCMS [3]. The certificate chains of EEs may be terminated by any RCA in the CTL.

The RCAs are administered by government or private entities. According to [3], an RCA operator can be a commercial entity, a common interest group, a national organisation, and/or a European organisation. In addition, each RCA can have jurisdiction per region (e.g. continent), sub-region (country-level), or even for an undefined region but rather a certain type or make of vehicle (i.e. vehicle OEM).

This TLM approach has the obvious drawback of a single point of failure, but the advantage of a more cost-effective deployment. This approach also provides the operational flexibility at the RCA level, so that multiple entities can operate RCAs and have them equally trusted via the CTL that the TLM signs.

3.4.2 Elector-based Trust Anchor Management Scheme

Electors, as described in [1], are cryptographic entities independent of the PKI. They can be operated at region-level and potentially be reused across regions. The regional authority decides which subset of the Electors are legitimate within their jurisdiction by identifying their certificates. Whenever the regional authority wants to add or remove an RCA or Elector certificate from their system, they ask at least a majority (n out of m) of these identified Electors to sign a ballot to endorse or revoke that certificate and add it to the list of previously issued ballots.

Just like Electors, RCAs could also be valid on a regional scale up to a global scale: they can be established following [14] with validity in a given jurisdiction being determined by the respective regional authority expressed through their respective list of ballots.

Electors belong in the policy domain of a V2X credential management system, while the RCAs belong in the operational domain. The policy domain includes the regional authority, which decides which RCAs to approve – in which case the Electors are simply cryptographic devices that uphold the policy decisions of the regional authority. To ensure fairness within the operational/business domain where the RCAs belong, Electors should not be operated by business entities that may have conflicts of interest.

3.4.3 Proposed Scheme for ESPS

The ESPS trust anchor management should thus be elector-based. This proposed scheme is depicted in Figure 4, where red boxes indicate central components that have only one instantiation per region, whereas green boxes indicate decentralised components that can have multiple instantiations per region. RCA “B” respectively Electors B and C are highlighted to demonstrate the reuse of an RCA respectively Electors on a global scale.

With this scheme, the ESPS would have a well-defined and standardised way to manage trust, even in the event of a compromise on the highest level. It would have a disaster recovery mechanism in place that is tested regularly by rolling over RCA or Elector certificates even in the absence of a disaster; with the benefit that at the EE level physical access is not required (i.e. no need to bring the EE in a secure environment for revocation and replacement).

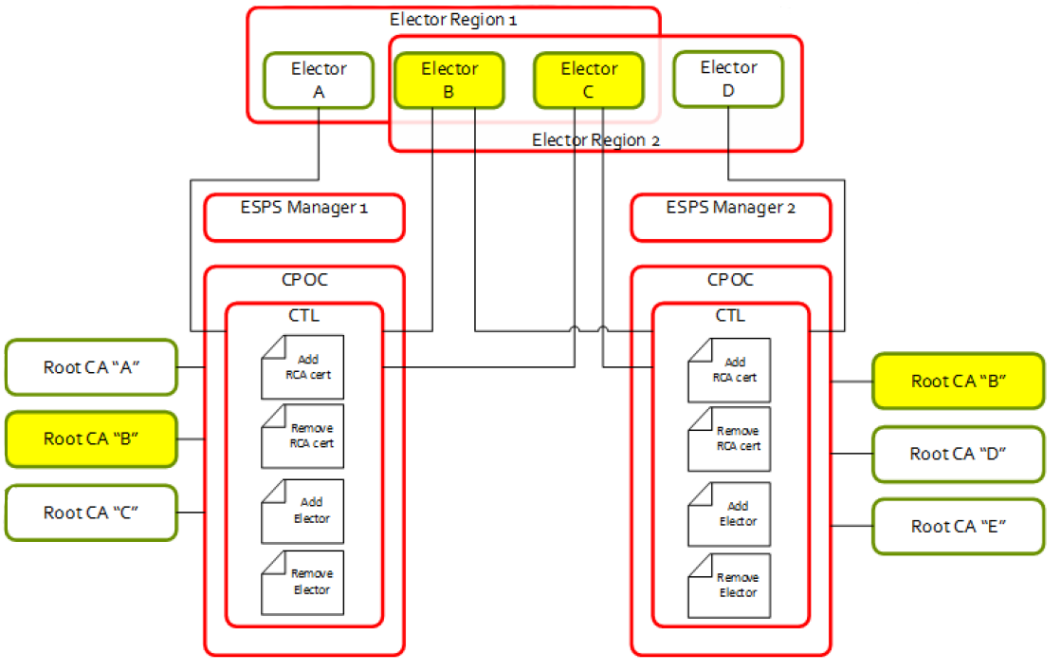

Figure 4: ESPS Trust Anchor Management Scheme

This proposal has several advantages:

- There is no single point of failure.
- The steps for regular rollover and disaster recovery after a compromise are the same from a device perspective.
- Electors could be reused across regions; therefore, it enables devices moving to a different region to obtain RCA and Elector information from peers via IEEE 1609.2 P2PCD.

To add Quantum Resistance (QR) to the previously introduced trust anchor system, over time each ECDSA (or other traditional PKI) signature can be accompanied by a corresponding QR signature. This is true for certificates, trust lists, and ballots – or use QR signatures from the very start.

4. Other Considerations

4.1 Distribution of CTLs and CRLs

Certificate Trust Lists (CTLs), as well as Certificate Revocation Lists (CRLs), have to be distributed to all EEs within the V2X PKI in the event a CA certificate or the certificates of an EE needs to be revoked. This could be done in four ways:

1. From a centralised Distribution Centre (DC), also called a Central Point of Contact (CPOC), that provides all Elector, RCA, and PCA certificates in one or multiple CTLs, and all CRLs to all EEs; **or**
2. Using a more decentralised approach, where each RCA is responsible for running its own DC, providing all CTLs and CRLs to EEs enrolled in its hierarchy, and providing its own CTL and CRL to other RCA DCs; **or**
3. Using a completely decentralised approach, where the CPOC provides a single CTL with RCA certificates only, and information about their respective DCs. After downloading that central list EEs connect to all of those DCs to download the respective RCA specific CTLs and CRLs; **or**
4. A peer-to-peer approach utilising IEEE 1609.2 P2P CD as defined in [14], where every EE is provided with just its own certificate chain, and whenever it comes across a message with an unknown certificate in its chain the EE would request verification (the certificate) from the sending EE – all certificate chains eventually end up in the same trust anchor(s).

The second approach is depicted in Figure 5. Red boxes depict central components that are only instantiated once, whereas green boxes depict decentralised components that can be instantiated multiple times. A Central CTL (CCTL) contains ballots to add or remove Elector and RCA certificates. This file is provided by the CPOC. Every RCA has its own DC, whose URL is provided in the CCTL entry for the RCA, and will publish its CTL, containing all the PCA certificates it issued, and its CRL via that DC. Each of those DCs will regularly check for an updated CCTL, and if there is an update (e.g. a new RCA) it will download and store that information, use the DC URL in the updated entry to download the other RCA's CTL and CRL, and check for updates of those two files on a regular basis. With that, each DC will always have all relevant CTLs and CRLs available. The EEs enrolled under the RCA will download all of these files from the RCA's DC.

Methods (1) to (3) provide lower latency for message validation compared to (4), in the event an EE does encounter a message with an unknown certificate in the chain. On the other hand, if devices in (1) to (3) did not update in time they might also encounter a message with an unknown certificate in its chain, although with C-V2X and cellular/mobile coverage, the chances might be significantly low. Nevertheless, it would be useful to always implement (4) as a fall-back option.

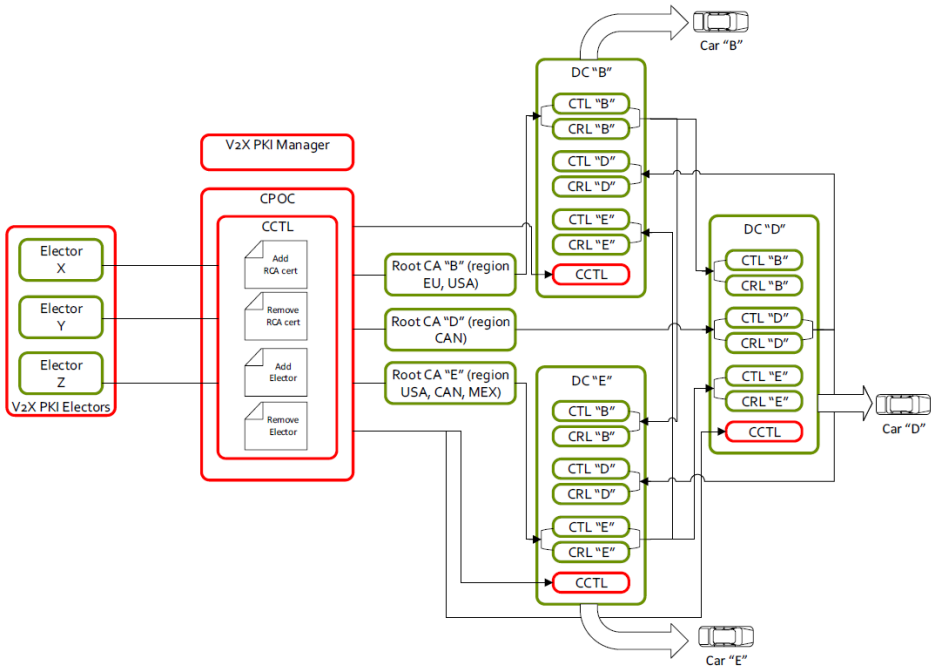

Figure 5: Decentralised Distribution of CTLs and CRLs

Evaluation

Each EE operator knows who is on its roster and knows the logic that determines the time those EEs will try to update CTLs and CRLs based on their programming. Individual operators are thus best placed to manage their own EE's demand for CTL and CRL updates. For this reason, we favour approach (2) with fall-back to (4), where individual RCAs (typically, although not necessarily, associated with individual operators) run their own DCs to distribute CTLs and CRLs. An additional advantage of this mechanism is that it does not reveal the number of devices sold by an OEM to any third party – which could be financially sensitive information.

5. Conclusions

To make V2X communications a reality, realising the societal and economic benefits that consumers and businesses have been expecting with the advent of 5G communications, it is paramount that the system architecture ensures not only the principles of security and privacy, but also those of deployability and practical operation. In this paper, we have motivated the update of privacy assumptions in the context of ubiquitous connectivity, as applicable to C-V2X-enabled End Entities and operational management principles governing complex systems. We have also described several simplifications of the security credential management systems. The results of this paper constitute a call to action for all V2X communication stakeholders to take these into account when implementing credential management systems for V2X. As for next steps, we aim to evaluate how to future proof such systems against possible threats that may arise as connected cars become ubiquitous.

6. References

[1] B. Brecht, D. Therriault, A. Weimerskirch, W. Whyte, V. Kumar, T. Hehn and R. Goudy, 'A Security Credential Management System for V2X Communications,' *IEEE Transactions on Intelligent Transport Systems*, vol. 19, no. 12, pp. 3850-3871, December 2018.

[2] Crash Avoidance Metrics Partners (CAMP) LLC, 'Security Credential Management System Proof-of-Concept Implementation; EE Requirements and Specifications Supporting SCMS Software Release 1.2.2,' [Online]. Available: https://wiki.campllc.org/display/SCP. [Accessed 1 August 2019].

[3] European Commission, *Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)*, vol. Release 1.1, 2018.

[4] IEEE P1609.2.1, *Draft Standard for Wireless Access in Vehicular Environments (WAVE) – Certificate Management Interfaces for End Entities*, 2019.

[5] ETSI, 'TS 102 940 v1.3.1 (2018-04) Intelligent Transportation Systems (ITS); Security; ITS communications security architecture and security management,' 2018.

[6] Crash Avoidance Metrics Partners (CAMP) LLC, 'Security Credential Management System Proof-of-Concept Implementation; Hardware, Software and OS Security Requirements,' [Online]. Available: https://wiki.campllc.org/display/SCP/Hardware%2C+Software+and+OS+Security+Requirements. [Accessed 2 August 2019].

[7] 3GPP, 'TS 33.220 Generic Bootstrapping Architecture (GBA).'

[8] US Department of Transportation (USDOT), National Highway Traffic Safety Administration (NHTSA), *Notice of proposed rulemaking (NPRM) Federal Motor Vehicle Safety Standards 150 (FMVSS-150); V2V Communications*, 2016.

[9] US Department of Transportation (USDOT), National Highway Traffic Safety Administration (NHTSA), *Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application*, 2014.

[10] ETSI, 'TS 102 941 v1.3.1 (2019-02) Intelligent Transportation Systems (ITS); Security; Trust and Privacy Management,' 2019.

[11] M. A. Simplicio, E. L. Cominetti, H. K. Patil, J. E. Ricardini and M. V. M. Silva, 'The Unified Butterfly Effect: Efficient Security Credential Management System for Vehicular Communications,' *2018 IEEE Vehicular Networking Conference (VNC)*, pp. 1-8, 2018.

[12] H. S. Ogawa, T. E. Luther, J. E. Ricardini, H. Cunha, M. Simplicio Jr. , D. F. Aranha, R. Derwig and H. Kupwade Patil, 'Accelerated V2X provisioning with Extensible,' *Cryptology ePrint Archive*, Report 2019/1039, 2019.

[13] Certicom, 'SEC 4 v1.0: Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV),' *Certicom Research*, 2013.

[14] IEEE, 'IEEE Std 1609.2-2016 - IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages,' *IEEE*, 2016.

[15] 3GPP, 'TS 33.501 Security architecture and procedures for 5G system.'

[16] 3GPP, 'TS 33.401 3GPP System Architecture Evolution (SAE); Security architecture.'


5GAA
Automotive Association