F2014-ACD-020

OPERATING A CAR-TO-X PKI – CHALLENGES FOR SECURITY AND PRIVACY

[1]Moser, Martin[*]; [1]Estor, Daniel; [1]Minzlaff, Moritz; [2]Weimerskirch, André; [3]Wolleschensky, Lars
[1]ESCRYPT GmbH – Embedded Security, Germany; [2]University of Michigan Transportation Research Institute, USA; [3]ESCRYPT Inc., USA

KEYWORDS –
Car-to-X Communication; Public Key Infrastructure; Automotive Security; Privacy

ABSTRACT –

An integral part of the security solution for a Car-to-X (C2X) communication system is a dedicated public key infrastructure (PKI) that creates the certificates used by the participants and thus establishes an anchor of trust within the system. However, this also raises new questions related to the operation of such a PKI. In this article we discuss these challenges and open issues as well as possible solutions and measures that enhance the security and protect the privacy of C2X participants.

TECHNICAL PAPER –

INTRODUCTION

Wireless communication between vehicles or related infrastructure (e.g., traffic lights, roadside units), C2X communication in short, is considered to take road safety to the next level. However, these safety goals cannot be achieved without proper measures to enforce security within the C2X system. Several solutions have been proposed which are based on digital signatures to ensure integrity and trustworthiness of C2X messages. Consequently, a public key infrastructure (PKI) needs to be established. The PKI consists of one or several certification authorities (CAs) which act as trust anchors in the system and provide certificates for ITS-stations by automated processes.
To protect privacy, on-board units (OBU) in vehicles need a medium to high number of short-term (pseudonym) certificates that they can change frequently to avoid being tracked. Furthermore, each station might also need a long-term / enrolment certificate that is tied to its identity. Therefore, a special PKI architecture needs to be used for a C2X environment. Two such architectures have been proposed by the respective stakeholders in Europe and in the US. While different, they also have many aspects in common.
One key area where both standardization as well as research have left many questions unanswered are the operational aspects of a C2X PKI. Questions within this area have strong implications on security and privacy and need to be answered before C2X comes to market. Examples are the following: Who should operate a CA? Should one organization be allowed to operate several CAs or even different kinds of CAs? How can the registration process for ITS-stations be managed securely and by whom? How can ITS-stations connect to the PKI and what does this imply? What are the implications of data collection and protection at the CA for the users' privacy?
In this article, we introduce both architectures and compare them to the state of the art research on C2X and non-C2X PKI systems. Furthermore, we investigate how well these

designs protect against potential security and privacy threats and identify challenges and open questions like those mentioned above. Based on this analysis, we derive strategies for a secure and privacy-protected operation of a C2X PKI.

STATE-OF-THE-ART PKI TECHNIQUES

Public key infrastructures have been used in non-C2X context for many years to secure the internet, e-mail communication, secure software flashing, and other use cases. Consequently, a number of state-of-the-art techniques have been established that improve the overall security and efficiency of the system.

On the one hand are measures that raise the cost of potential attacks. Noteworthy in this category are hardware security modules (HSM) that provide physically secure environments for storing and using cryptographic keys, two-factor user authentication [1] at least for critical roles such as administrators of a CA, a 4- or 6-eyes principle for critical tasks, and certificate pinning to detect man-in-the-middle attacks [2]. On the other hand are techniques that limit the potential damage of a successful attack. Misbehaving participants of a PKI can be excluded from the system through revocation (more on that below) and secure communication channels should integrate so-called "forward secrecy" so that should an attacker gain knowledge of the encryption keys used at a certain moment in time, they do not gain any knowledge about past data transmissions [3]. Similarly, certificates can precisely define the allowed use cases for a given key so that abuse of a stolen key is limited to the initially intended use case.

In terms of efficiency, some other trends are gaining momentum. Two techniques that reduce the memory footprint of a PKI in embedded devices are noteworthy: The card verifiable certificate (CV certificate) format can be an alternative to the X.509 format and elliptic curve cryptography (ECC) offers a comparable level of protection as RSA cryptography with much shorter key lengths [4].

Finally, particularly in a PKI for C2X, the demand for strong privacy drives many architectural design decisions and influences the content, distribution, and revocation of certificates. Some of these considerations are discussed in the following.

Number of certificates in a vehicle

Typically, digital certificates are used to verify the sender's identity. In C2X communication, however, the actual identity of the sender is not required to ensure trustworthiness of a message but it suffices to verify that a message has been sent by a valid C2X participant. Thus, certificates must not contain any content that links them to a particular vehicle or owner in order to keep privacy. For example, a certificate should not contain a vehicle's VIN. However, if a vehicle only uses a single certificate during its lifetime, then this certificate can be used to track the vehicle and still compromise vehicles' privacy – regardless of whether the certificate contains any information about the owner. This means that an attacker who observes the certificate at different locations can reconstruct the movement of the vehicle. So the vehicle needs to have a set of multiple certificates. There a various approaches: In the safety pilot project [5] overlapping certificates are used. Every certificate is valid for 5 minutes with 30 seconds overlap to enable smooth transition. The vehicle will never use the same certificate twice (called approach A). In [6], a different approach is used which is currently also favoured in the EU. A vehicle receives a set of certificates (e.g., 20) for a certain time period (e.g., a week) and can switch between them at will. This implies that during a single week the same certificate might be used multiple times, so this could compromise privacy (called approach B). Note that in both approaches the used certificates are not linkable by an observer without

special knowledge (see Section "Revocation"). These different approaches show that a balance between privacy, usability, and system cost needs to be found. In Approach A the vehicle uses 2016 certificates per week, in Approach B the vehicle uses significantly less certificates per week (e.g., 20). Approach B uses less memory in the vehicle and saves cost. However, if an attacker is able to extract certificates from the vehicle, sibling attacks (attacker extracts certificates to impersonate multiple vehicles at the same time) are possible. Approach A limits these attacks to 2 siblings at the same time (during the 30 second overlap) whereas Approach B allows for simultaneously active 20 siblings every week. Both approach A and B are configurable by varying either the lifetime of certificates or the number of certificates.

Revocation

It might become necessary to remove bad actors from the system. This requirement influences the PKI design. On the architectural side there needs to be a mechanism to detect misbehaving actors, e.g., there must be a communication channel to the PKI for reporting suspicious behaviour. Once a bad actor is identified, it needs to be removed from the system. Different approaches for removal of bad actors exist.

Certificate Revocation List (CRL)

One idea is to publish bad actors on a CRL. This is an often used and for traditional PKIs standardized approach. The disadvantage is that CRLs need to be distributed to every vehicle in a timely manner. Different optimizations exist. Delta CRLs are published frequently but each CRL contains only the newly revoked entries in comparison to full CRLs. This has the advantage that instead of a single large CRL several small CRLs are used. The disadvantage is that if a delta CRL is missed by a vehicle there needs to be a way to request this particular CRL. Another approach is to use regional CRLs. Instead of having one small CRL for the whole system it is divided into several regions, e.g. a CRL for the west coast of the US and one for the east coast. Again, this approach reduces overall CRL size but has the disadvantage that an attacker that moves between regions needs to be revoked in every region.

Privacy is also affected by CRLs. If a vehicle is on a CRL it could possibly be tracked by its revoked certificates, e.g., if a single vehicle is revoked in a given neighbourhood, then it can be tracked by its revoked messages. A simple countermeasure is that if a vehicle detects itself on the CRL, it stops transmitting messages. Another issue with CRLs is efficiency. If a vehicle possesses multiple certificates that are unlinkable, every single certificate needs to be put on the CRL which increases the bandwidth requirement. This problem was overcome in [7] by the usage of linkage values. This approach also covers the use case of stolen or sold vehicles. If the thief or new owner misbehaves it should not impact the privacy of the previous owner.

System Exclusion

Another approach is to provide vehicles with a limited set of certificates and force re-provisioning at certain intervals. Bad actors are removed from the system by not being re-provisioned with new certificates. This has the advantage that no CRLs are needed, but there is a slow reaction time equivalent to the validity period of certificates.

STANDARDIZATION OF C2X PKI STRUCTURE IN EU AND US

In this section we present the current state of the various standardization and design efforts in both Europe and the US. We describe the commonalities and differences in the following.

Architecture

Certificates are issued by central components of the PKI. If no special care is taken then insiders of these components can track which certificate is issued to which vehicle, i.e., an insider at the PKI knows exactly which certificates are stored in which vehicle. In [8] a PKI design was suggested to mitigate the issue. The PKI is split into several different components. In order to undermine the privacy of a vehicle, two of these components need to collude. It would be possible to give different components to competing companies or different government branches to reduce the chance of cooperation. However, there could still be legal processes to force cooperation and reveal the identity of a vehicle by its certificates if the need arises.

At this time, both Europe and the US consider a C2X PKI but did not standardize its design. It might actually be the case that only some aspects are standardized. In the US, the interface between OBU and C2X PKI will likely be standardized whereas in Europe, OEMs might use proprietary OBU to PKI interfaces. Both Europe and the US will have to define requirements and the architecture of a C2X PKI. Both also consider a PKI for C2X vehicle safety communication applications. The plans for a US C2X PKI were published in [7] and [8], and plans and interface for a European C2X PKI were presented in [9] and [6].

The European C2X PKI mainly consists of a root certificate authority (RCA), a long-term certificate authority (LTCA), and a pseudonym certificate authority (PCA). The RCA issues certificates for LTCA and PCA and controls policies. The LTCA issues a long-term certificate that enables devices to request pseudonym certificates (PCs), and the PCA issues the actual pseudonym certificates.

The C2X PKI foreseen in the US comprises a root CA, an enrolment CA (ECA), a registration authority (RA), a pseudonym certificate authority (PCA), two linkage authorities (LA), and several other components. The ECA allows enrolment of devices and issues an enrolment certificate that a device then uses to request short-term certificates. The RA receives such requests from the devices, the PCA issues pseudonym certificates, and the LAs generate so called linkage values to enable efficient revocation via CRLs.

Privacy

In the US, it is expected that C2C safety communications will be introduced as a mandatory safety technology in all vehicles. Therefore, the US design prioritizes protection of users' privacy. Privacy protection includes protection against 3rd party sniffers and against inside attackers, such as rogue employees but also institutional attacks. The US design accounts for outside and inside attackers at a level that at least two institutions need to collude in order to compromise users' privacy, i.e. there is a technical privacy protection included such that organizational protection can easily be implemented. The European C2X PKI allows implementing privacy to the same level. However, there are fewer technical restrictions against inside attackers but such protection needs to be implemented on an organizational level. Note that both PKI designs allow a parameterization to account for privacy protection against outside attackers by allocating pseudonym certificates for a certain time-period that are regularly changed by on-board units.

Scope

The scope of a C2X PKI could be for both Car-to-Car (C2C) applications and Car-to-Infrastructure (C2I) applications, or it could be for C2C applications only with another PKI for C2I applications. Both solutions are technically feasible. In the first setting, there is a single root CA that issues sub-CA certificates for a C2C and a C2I CA that in turn issue

pseudonym certificates and certificates for RSUs. This approach is currently favoured in Europe. In the second setting, there is a root CA for C2C applications and another root CA for C2I applications. Both root CA certificates are loaded in each OBU and each RSU via a trusted channel, e.g., as part of the firmware and then each device is able to verify messages that were sent from either OBU or RSU. It is even possible that there is not a single root CA for C2C or C2I applications but that there are several root CAs for either category. For instance, there might be a root CA for C2C safety applications and another root CA for C2C mobility applications. Again, this is feasible as long as all root CA certificates are loaded to OBUs and RSUs via trusted communication channels. Using a single root CA provides the highest level of control and allows the root CA to enforce its policies to all sub-CAs. Using several root CAs provides a higher level of flexibility. Note that work is on-going in the US to determine the preferred approach.

Policies

The US PKI introduces an authority called "SCMS Manager" that defines and enforces policies for the PKI. Policies can be enforced for SCMS components and for devices. The SCMS manager has control over SCMS components by defining the policies for issuing CA component certificates (e.g. for issuing a sub-CA certificate for Registration Authority or Pseudonym Certificate Authority). The SCMS manager will also define the policies for device certification by defining requirements to receive an enrolment certificate in the first place, i.e. the requirements to receive certificates can be used to enforce minimum performance and quality levels of OBUs and of RSUs.

OPERATING CHALLENGES

In this section we present the most important challenges for the operation of a C2X PKI and discuss possible solutions with respect to their advantages and disadvantages.

Different Operator Models

A major issue in PKI operation is the question of the actual operator of a CA. The PKI can be operated by a government organization, by a private company or a consortium of such, or by a public-private partnership. In the US it is likely that a public-private partnership will operate the C2C PKI for safety applications. The PKI can be under control of a single operator, or control can be separated. In the latter case, the PKI components are technically and organizationally separated. The separation can be within an organization, or it can be a stronger separation by providing control of individual components to different organizations. Both European and US PKI allow such separation. Note that the US PKI introduces a variety of components and allows separation to a higher degree. Finally, we have to distinguish between two positions: The operator in charge, i.e. the responsible institution which instructs, controls and also pays the CA operation, as well as the technical operator, i.e. the institution which actually implements, operates and maintains the CA.

Operator in Charge

For the root CA, the operator in charge must be an industry-wide accepted institution, e.g. a consortium of all OEMs or a governmental body. Natural operators in charge for the other CAs are the OEMs, as they offer the C2X functionality as a benefit to their customers and they have insight into all the technical details of the C2X implementation in their vehicles. Of course, groups of OEMs forming a legal entity are also possible. In theory, governmental

bodies may also operate the long-term/registration CA, as they already have an existing body for the registration of vehicles. However, it is questionable whether these bodies do have the technical know-how for the installation and operation of a CA, left alone the questionable governmental interest in such expensive involvements. Therefore, a public-private partnership may be preferable to this solution.

Technical Operator

Of course, an obvious choice for the technical operator is the operator in charge itself. Besides this, it is also possible to assign the technical operation to an external supplier of CA/PKI services with expert knowledge in the field. This may have several advantages. First, the supplier will offer the service to more than one customer with the synergy effects resulting in significantly lower cost and implementation time (assuming that a ready-to-use implementation already exists). This will be particularly true for special services such as 24h world-wide support, guaranteed availability, special security hardware or established processes. Furthermore, such solutions can achieve a considerably higher level of quality and security due to the expert knowledge and implementations hardened by the use at many different customers throughout many different areas (bug-tracking, regular updates etc.).

Registration Process

A huge operational issue is the registration of vehicles which we will sketch at this place only for the European architecture. However, the adaption to the US design is trivial.

In order to request certificates from the PKI, a vehicle and its module authentication public key must first be registered at the long-term CA (LTCA). This is not trivial, since it involves several parties (in addition to the LTCA at least the OEM and the supplier of the security module). It must be ensured that all devices and parties participating in the communication scheme adhere to a minimum level of quality and security. This forces the PKI to perform some sort of evaluation (self-evaluation might be possible) before provisioning a device / device type with certificates. Moreover, it has to be taken close care that the C2X registration does not interfere with the normal production process, as a delay or stop of the production line always results in enormous cost.

After registration, it might be necessary to reissue certificates to a vehicle in the field, for example for re-provisioning as discussed above. This can either be done at an authorized dealership (e.g. during vehicle maintenance) or over the air. In both cases certificates need to be transmitted confidentially from the PKI backend to the vehicle. Taking this into account, we propose the following two possible registration procedures.

Vehicle-Based Registration Process

In the vehicle based registration process, the supplier first produces and initializes (i.e., generates a module key pair) the security module. In the next step, he delivers the security modules (identifiable by serial numbers) and, separately through a secure channel a digital list of the public module authentication keys in combination with the serial numbers. The OEM can mount the security module into the vehicle and independently register the module with its public key at the LTCA. The car can then automatically request certificates and is fully equipped upon delivery to the customer. If the OEM does not operate the LTCA himself (see also previous section), he needs a secure registration interface to it.

One of the main advantages of this process is that the registration is completely independent of the production, i.e. a failure of the registration or downtime of the PKI will not delay or stop the production line. Furthermore, the car and its C2X components are already fully functional upon delivery to the customer. Another advantage is that the OEM retains control

over the registration process and flaws like the injection of false public keys will be detected. In case of such an attack, the originally registered car will not be able to request certificates as only one key is registered for every mounted security module. Hence, the falsely registered public key can be easily deregistered at the LTCA.

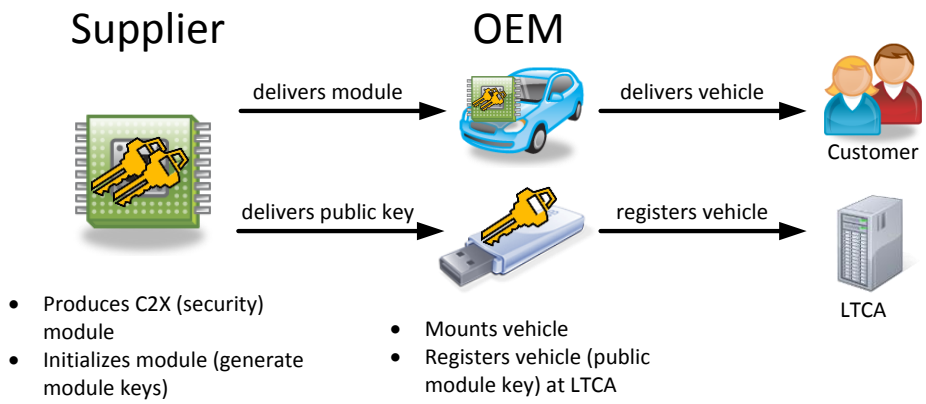

Figure 1 Vehicle-based registration process

Owner-Based Registration Process

In contrast to the vehicle-based process, here the OEM does not itself register the vehicle, but delivers the public key to the customer together with the vehicle itself. The customer can then register the vehicle at a local authority which acts as a proxy to the LTCA.

Here, the registration is bound to both, the vehicle owner as well as the vehicle itself. This can have advantages in case of detected misbehaviour. Furthermore, the same advantages with respect to independence of production and detection of falsely injected keys also apply here. The big drawback of this solution is that the process causes additional efforts for the customer and the C2X modules will not be functional when the vehicle is delivered. This may not be acceptable for OEMs and customers.

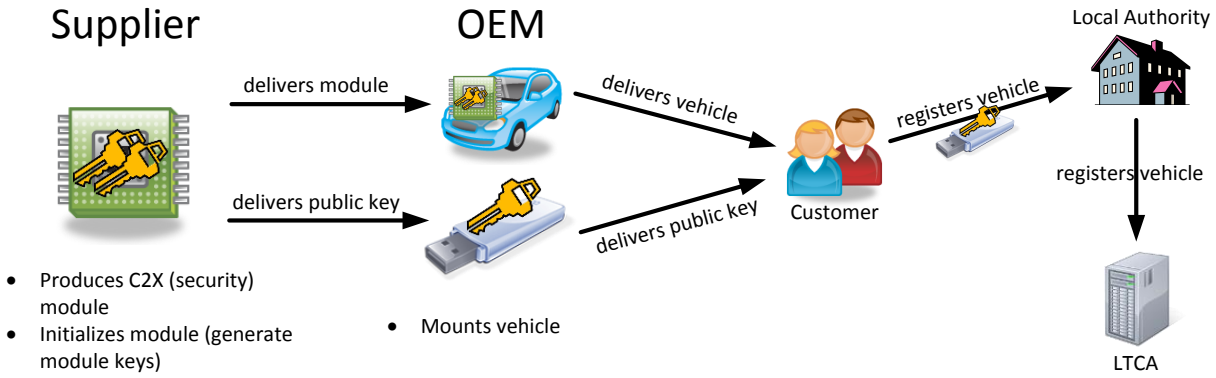

Figure 2 Owner-based registration process

Rights and Permission Management

Rights and permission management at a C2X PKI must consider usage rights and access control for human actors at an operator as well as permission management for the registered C2X participants. While separation of duties in the complete PKI domain is given by the design stipulating a split into different components, the operator of each component has to take additional measures to ensure a proper access control in the respective component. As

established in classical PKI, access control inside one CA or registration authority, can be realized by the introduction of different roles such as a user administrator who manages people or organizations that are allowed to register ITS stations, an auditor who may view the PKI logs, a developer who implements the CA application and a system administrator who takes care of the server infrastructure. As a C2X PKI provides a machine-to-machine interface for certificate requests, a dedicated role for participants is required to authorize access to these interfaces. Another aspect of permission management, which is specific to a C2X PKI, is the use of specific permissions for sending certain kinds of messages, which are encoded in the respective certificates [9] and [10]. While the encoding of permissions in certificates is specified, the content and the set of possible permissions is yet to be defined.
Permission management does involve much more than just storing the permissions in one common database table. Instead, several issuance policies have to be enforced, covering the complete lifecycle from setup of a CA until issuance of pseudonym certificates. At the first step, an authenticator may be restricted to register only certain permissions for its C2X participants. For example, the permission to use the blue light or priority at traffic lights must only be registered by certain, possibly sovereign authorities, while an OEM must only be allowed to register permissions for certain message types such as CAM or DENM messages, or certain infrastructure-related permissions may only be registered by operators or manufacturers of these devices. At the next step, during the registration of the vehicle or more general the ITS station, the respective permissions have to be chosen and stored in the database entry of the newly registered entity. Since some C2X participants may require certain sets of permissions – think of a plain clothed police car that is exposed as police car in an emergency situation – it is practical to define permission profiles that collect certain sets of permissions. Finally, these permissions have to be enforced during issuance of both long-term and pseudonym certificates. There could be profiles for a normal car, police car, ambulance, public transport, traffic light, further infrastructure, etc. Not only must the requested permissions be a subset of the allowed permissions stored for the requesting entity, also the issuing CA may be restricted to issue only certain kinds of permissions and must reject a request if it is not authorized to issue a certificate with a requested permission. As the authorized permissions of a CA are stored in its CA certificate, a long-term or pseudonym certificate will be invalid if a CA issues certificates without being authorized to do so.

Privacy Issues

The immediate and most obvious threat to privacy concerning the operation of a C2X PKI is an insider reading and evaluating the available data. The system architectures proposed for the US and Europe in [7] and [6] already contribute significantly to protection against such attacks in technical terms. When it comes to actual operation of a PKI, however, there are further issues that have to be addressed. While the concepts foresee a technical separation of different PKI authorities, it is not precluded that multiple authorities be operated by one organization. This is not necessarily a problem as long as the operator establishes appropriate policies that prevent, for example, one person from being able to access information at more than one component of the PKI. However, this possibility has the potential to seriously weaken the technical privacy protection measures and hence has to be considered carefully when it comes to actual operation of a C2X PKI.
Next, there is the question which data are collected by a CA operator. Every request at the CA generates connection information related to the requester such as IP address or TLS certificates. While there seems to be no immediate problem with storing such information, there may be situations where this information can be used to harm privacy. For example, workshops or roadside equipment that act as proxies for certificate requests could later be

used to map a certificate to the real identity of the vehicle, e.g., by evaluating the workshop's appointment schedule. However, note that such threats can be countered by introducing a location obscurer proxy (LOP), as is foreseen in the US PKI design. Furthermore, the audit log of the CA operator generates information about its employees. As information which is not stored cannot be abused, it always has to be weighed thoroughly what information is stored. These considerations also must include national and, if applicable, international data protection laws.

Finally, there are several aspects regarding the certificate issuance process that might leak information about requesters of certificates. By design, a pseudonym certificate always contains information about the CA that issued the certificate. If the number of certificates is large, this is not a problem with regard to privacy because during a journey, there will most likely circulate messages of other vehicles whose certificates were issued by the same CA. If, however, a CA only issues certificates for a small number of different vehicles, it may be easily identified which pseudonym certificates belong to one vehicle. This linking of certificates becomes even easier, if it is known that a certain CA is operated by an OEM and it is known that this CA only issues certificates for its own vehicles. Other information contained in certificates such as permissions and validity dates could also allow linking of pseudonyms. If the permissions in issued certificates are too specific, pseudonym certificates of the same vehicles could be identified just by the characteristic set of permissions. If the CA always takes the current time as basis for the certificate validity periods, certificates can easily be distinguished by their validity periods. This collection of potential information leaks that are caused by an unsuspecting issuance policy is not complete, but it points to questions that have to be thought of in a continuous process.

Auditing of C2X PKIs

As the participants in a PKI build their trust in the system on the fact that its CAs are honest and uncompromised, this raises the question of how to establish and maintain the trust in theses CAs. The typical solution consists of audits that verify that the CAs implement a high standard of operational and technical security. The established approach is for a CA to declare that it follows a so-called certificate policy (CP) or certificate practice statement (CPS) as defined in RFC 3647 [11]. These documents not only include guidelines for how the CA is to be operated, but also addresses questions regarding the audits themselves. It specifies when an audit needs to take place, who can take the role as auditor, what an audit needs to cover, and the consequences of an audit.

An obvious trigger for an audit of CAs (e.g., LTCA, PCA, or RCA in Europe) is the moment before their CA-certificate is issued or re-issued. It is therefore possible to regulate a minimum frequency of audits through the lifetime of certificates. Similarly, ITS-Authenticators should be audited whenever they are (re-)registered. In addition, every time breach of trust or misuse is suspected, the need for an audit may arise. Whether an audit is actually required after a suspicion has been voiced, may be up to the individual auditor.

An immediate choice for the auditor is the issuing authority, e.g. the operator of the RCA for audits of an LTCA, or a financially and organisationally independent, trusted third party. The case of the RCA is special as it issues its own certificate but must not audit itself. Possible choices for a trusted third party as auditor include a governmental agency, a company of security experts, or, similar to a Common Criteria certification, a combination of both where one party carries out the audit itself and the other checks that the audit process is proper.

The items that the audit needs to cover are written down in a CP or CPS. They should cover access control, hardware and software maintenance processes and generally all aspects raised in this paper so that, e.g., it is ensured that the CA/ITS-Authenticator employs state-of-the-art

techniques. Clearly the CP/CPS assumes an important role in the auditing process and thus should be carefully written, e.g. with the help of security experts.
If an audit is successful, then a certificate is issued or registration takes place. No other immediate actions are necessary. If a CA/ITS-Authenticator fails an audit, then the situation is more complex. Obviously, its certificate/registration is not renewed. In addition, the current certificate/registration should be revoked and the revocation be communicated to the C2X participants.

CONCLUSION

The challenges for the operation of a C2X PKI are manifold which is not surprising for such a new and dynamic field. As an integral part of the C2X security solution, these challenges need to be overcome with dedicated measures, policies and implementations. As we have shown in this paper, some dedicated research is already going on with respect to this topic and solutions can be found which we have presented in the different sections.
Of course, there is still a lot of work to be done to establish these solutions, but with the joint effort of researchers, OEMs, suppliers as well as experts on security, C2X communication and PKI operations, it will be possible to solve the open issues, successfully operate C2X PKIs and bring C2X to the market.

REFERENCES

[1] J. Tarala, „Two-Step Verification," *OUCH! magacine,* 2013.

[2] J. Walton, „Securing Wireless Channels in the Mobile Space," in *OWASP Virginia Chapter*, 2013.

[3] W. Diffie, P. C. Van Oorshot und M. J. Wiener, „Authentication and authenticated key exchanges," *Designs, Codes and Cryptography,* Bd. 2, Nr. 2, pp. 107 - 125 , 1992.

[4] N. Sullivan, „A (relatively easy to understand) primer on elliptic curve cryptography," 2013. [Online]. Available: http://arstechnica.com/security/2013/10/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/.

[5] Safety Pilot Model Deployment, [Online]. Available: http://www.safetypilot.us/.

[6] N. Bißmeyer, H. Stübing, E. Schoch, S. Götz, J. P. Stotz und B. Lonc, „A Generic Public Key Infrastructure for Securing Car-To-X Communication," in *ITS World Congress*, 2011.

[7] W. Whyte, A. Weimerskirch, V. Kumar and T. Hehn, "A Security Credential Management System for V2V Communications," in *IEEE Vehicular Networking Conference (VNC)*, 2014.

[8] T. Hehn, "A Security Credential Management System (SCMS) for Vehicle-to-Vehicle Communications," in *ESCAR USA*, 2013.

[9] European Telecommunications Standards Institute (ETSI), „TS 103 097: Intelligent Transport Systems (ITS); Security; Security header and certificate formats," V1.1.1, 2013.

[10] Institute of Electrical and Electronics Engineers (IEEE), „IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages," 2013.

[11] Network Working Group, „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework," 2003. [Online]. Available: https://tools.ietf.org/html/rfc3647.