Security Issues for Future Intelligent Transport Systems

Ernest, Foo[a], Christopher, Djamaludin[a] and Andry, Rakotonirainy[b]

[a] School of Electrical Engineering, Computer Science, Information Security
[b]Centre for Accident Research and Road Safety Queensland
Queensland University of Technology

Abstract

Cooperative Intelligent Transportation Systems (C-ITS) allow in-vehicle systems, and ultimately the driver, to enhance their awareness of their surroundings by enabling communication between vehicles and road infrastructure. C-ITS are widely considered as the next major step in driving assistance systems, aiming at increasing safety, comfort and mobility for drivers. However, any communicating systems are subjected to security threats. A key component for providing secure communications at a large scale is a Public Key Infrastructure (PKI). Due to the safety-critical nature of Vehicle-to-Vehicle (V2V) communications, a C-ITS PKI has functional, performance and scalability requirements that differ from traditional non-automotive environments. This paper identifies and defines the key functional and security requirements for C-ITS PKI systems and analyses proposed C-ITS PKI standards against these requirements. In particular, the proposed US and European C-ITS PKI systems are identified as being too complex and not scalable. The paper also highlights various privacy, security and scalability concerns that should be considered for a secure C-ITS PKI solution in the Australian transport landscape.

Introduction

Connected systems and (semi) autonomous vehicles will be the hallmark of the future generation of Intelligent Transport Systems (ITS). In the US, assuming a full market penetration, connected vehicle safety applications could potentially prevent 25,000 to 592,000 crashes, save 49 to 1,083 lives, avoid 11,000 to 270,000 Maximum Abbreviated Injury Scale (MAIS) 1-5 injuries, and reduce 31,000 to 728,000 property-damage-only crashes annually (Harding et al., 2014). Vehicles' safety and mobility functionalities are increasingly reliant on software and wireless communications. Dedicated Short Range Communication (DSRC) is predicted to be the defacto standard supporting inter-vehicular communications. Vehicle-to-Vehicle (V2V) equipment and supporting communications functions could cost approximately US$341 to US$350 per vehicle in 2020 (Harding et al., 2014). The future environment of C-ITS will be characterised by highly mobile cars, a dynamic network topology with extremely short connections, variable network reliability and lower computing power relative to the desktop counterpart. The pervasiveness of DSRC will make on-board safety software vulnerable to cyber attacks.

To protect V2V communications, particularly safety critical messages, authentication is required. The Internet uses public key cryptography and digital signatures to provide authentication. Public key cryptography requires that each entity has a private key that is only known to the owner of the key and a public key that is distributed to all message receivers. A message sent to the receiver also contains a digital signature of the message and a certificate that contains the public key of the sender. Figure 1 depicts the process of signing and verifying messages using public key cryptography. The sender's public key is used to verify messages that can only be created by the sender's private key. The problem is that if a public key is incorrectly labelled, then the receiver can verify a message and mistakenly think an invalid message is correct. A PKI contains a distributed

system of certificate authorities. The Certificate Authority (CA) in a PKI as shown in Figure 1 distributes and vouches for certificates that contain the public keys of all the entities in the system.

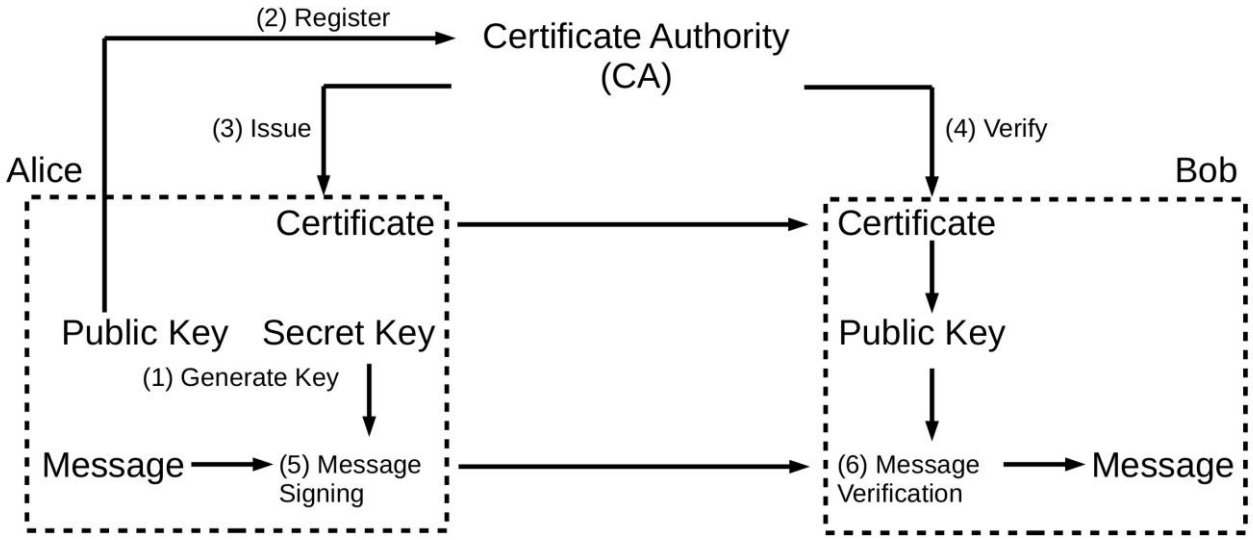

Figure 1. Signing and verifying a message using a certificate authority PKI

The impact of a compromise of the C-ITS PKI will allow attackers the ability to inject, modify and replay messages. Safety critical and traffic management messages can be falsified to cause vehicle collisions. Attacker vehicles may be able to create false identities and masquerade as emergency vehicles, thereby getting preferential treatment in traffic or send false information to vehicles to cause traffic jams and to free other roads from traffic.

The contribution of this paper is the definition of C-ITS PKI security requirements. A critique of the European Union (EU) (Bissmeyer et al., 2011) and United States (US) (Whyte et al., 2013) proposed C-ITS PKI standards is conducted and shows that neither standard fully meets the requirements set out in this paper.

This paper is constructed as follows. The next section defines the C-ITS PKI security requirements and an attack model required for C-ITS PKI systems. The third section describes the certificate provisioning and revocation processes in the EU and US standards. Following on, the fourth section analyses these two standards according to the security requirements and the final section provides a discussion and final thoughts regarding an Australian C-ITS PKI standard.

Security Requirements and Attack Model

A C-ITS PKI security requirement describes the properties that such systems should achieve. Security requirements are always described in conjunction with an attack model. The attack model defines what threats the security system should be able to protect against and the abilities of the adversary or attackers that the system is expected to defend against.

Security Requirements

Security requirements for C-ITS PKI are related to certification and validation, privacy, scalability and efficiency and revocation.

Certification and Validation

Certification and validation are the key properties of a PKI, and provide supporting security assumptions to the cryptographic algorithms and protocols used in the C-ITS. A certificate contains the public key that belongs to an entity in the system that is signed by the certificate authority. In the C-ITS all vehicles and roadside infrastructure that communicate to each other will all require certificates. The certificate is used to ensure that the public key that is received with a message belongs to the correct entity. Without certification, an attacker may be able to substitute their own public key for another entity and send messages claiming to be from that entity. If a PKI possesses the certification and verification property, the system should be able to successfully distribute and verify public key certificates belong to the correct entities.

Privacy

One of the key requirements of a C-ITS PKI is that the privacy of the car is maintained. There are two aspects of privacy. First is operational privacy. Operational privacy describes situations where cars need to be anonymous from other cars and roadside infrastructure. It is expected that cars should be anonymous while they are sending and receiving messages in normal C-ITS operations. Second is the desire for car to be anonymous from the certificate authority and the other components of the C-ITS system that make up the certificate distribution system. This second level of anonymity is much harder to achieve and requires complex systems and protocols to maintain.

Revocation

One of the key functions of a PKI system is the ability to maintain trust and security by notifying nodes of invalid or corrupted certificates. A mechanism must exist that allows the entities to recognise that the central authority no longer accepts a particular public key. This is a necessary function, as it cannot be assumed that secret keys and their associated public keys can be kept secure indefinitely. The revocation system is one that becomes problematic as the system grows. It is challenging to ensure that all system participants have up to date certificates and keys.

Scalability and Efficiency

The C-ITS PKI described in this paper are large scale infrastructures that are intended to span continents in terms of geographic scope. The means that the number of vehicles using the system is expected to run into the hundreds of millions. This is a challenge as the only other PKI system that is similar in magnitude is the one provided on the Internet. As a result of the massive scale of the PKI, all computations, communications and storage usage should be carefully considered. Part of this requirement is that these performance metrics do not place a burden on the system. The vehicle communication system must be functional despite the PKI system used to secure it. One of the other key factors in the scalability requirement is the speed which authenticated messages can be computed, transmitted and verified. Messages warning of collisions and other safety related events must be delivered with enough time to spare for a human driver to act on the contents of the message.

Attack Model

Our attack model is based on standard information security attack models for wireless sensor networks (Alzaid et al., 2008).

Attacker Abilities

Given a wireless V2V communications medium, it is assumed that the transmission medium cannot be physically protected from the attacker. The attacker is capable of viewing all messages transmitted across the network between the car and the PKI authority servers. In addition, the attacker should be able to inject, modify and replay any messages that it has encountered before. The attacker has full control of the network between the PKI authority servers and the car.

Attacker Behaviour

The aim of the attacker is to undermine or prevent the security properties previously described from being provided. In terms of privacy, an attacker will seek to determine the true identity of the car and link the car to multiple operations or locations in the PKI system. In terms of certification, the attacker would like the car to accept an invalid or previously revoked public key certificate.

Target Vulnerabilities

It is also possible that the attacker is able to gain control of the in-car Controller Area Network (CAN) bus. Thus the attacker may be able to control aspects of this network. However, it is assumed that the long-term private keys and session keys used in the PKI are stored on board the car in a secure storage facility such as a Trusted Platform Module (TPM).

C-ITS PKI Standards

This section will describe generic C-ITS PKI schemes that are the core of the EU (Bissmeyer et al., 2011) and US standards (Whyte et al., 2013).

EU Standard

The Car-2-Car Communication Consortium (C2C-CC) is a EU industry forum on car-to-car and infrastructure communication technologies. This forum presented a PKI organisation and structure that issues certificates to car to other device (C2X) enabled units. The PKI was specifically designed to have minimum overhead and maximum scalability while preserving privacy.

The C2X PKI consists of three main stationary authority entities: the Root Certificate Authority (RCA), the Long Term Certificate Authority (LTCA) and multiple Pseudonym Certificate Authorities (PCA). These authorities interact with typical ITS endpoints that include cars, ITS central traffic management stations, or ITS roadside stations. For the purpose of our paper all of the ITS endpoints can be considered to be the same and are referred to as cars.

Certificate Provisioning

The RCA is the central trust anchor that is responsible for establishing the trust of multiple LTCAs and PCAs. The LTCA is responsible for issuing a Long Term Certificate (LTC) to each car. The certificate will identify and authenticate each node in the system but it is not used for wireless communication. The PCA is responsible for issuing pseudonym certificates that are used for wireless communications. The car sends a certificate request to the local PCA. The PCA forwards

the request to the LTCA if it is in the correct jurisdiction for the LTCA. Otherwise the request is forwarded to another PCA. The LTCA verifies whether the car is allowed to exist on the network, and instructs the PCA to issue a signed pseudonym certificate to the ITS. The EU Certificate Provisioning scheme presented uses the PCA to obscure and therefore provide privacy between the ITS and the LTCA.

Certificate Revocation

The EU standard for certificate revocation does not rely on Certificate Revocation Lists (CRLs). The system relies on the Registration Authority (RA) or other entity to report the revocation of a car's certificate to the LTCA. The LTCA records the status of the car and waits for a pseudonym request from the PCA. The LTCA checks the status of the car each time a pseudonym certificate is requested and then rejects the certificate if the car is to be revoked.

US Standard

The US Department of Transportation has also recommended a V2V communications PKI called the Security Credential Management System (SCMS). In comparison with the EU Standard, the US standard is far more complex. The SCMS requires up to five authority servers and ten message communications to complete the certificate provisioning protocol. The authority servers include a Linkage Obscurer Proxy (LOP), Registration Authority (RA), two Linkage Authorities (LA_1, LA_2) and a Pseudonym Certificate Authority (PCA).

Certificate Provisioning

To get a certificate, the car must first send the certificate request to the LOP which will obscure any identifying details of the request such as the location details and forward it on to the RA. If the request is valid, the RA will send an acknowledgment back to the car. However, the RA does not immediately send back the requested certificates to the car even though an acknowledgment message is returned to the car. Instead the RA waits for a number of requests before proceeding to hide the identity of requesters from the PCA. To create a pseudonym certificate, the RA collects encrypted keying material pre-linkage values from LA_1 and LA_2 and includes them in the request to the PCA for a pseudonym certificate. Two linkage authorities are required so that no single linkage authority may hold the linkage values for a particular device, and thus be able to track it. The PCA sends the pseudonym certificate containing the public key and hash of the certificate to the RA. As part of the pseudonym certificate the PCA obscures the pseudonym certificates to ensure that the RA is not able to recognise any pseudonym public keys that it is distributing. The RA returns the collected super-batch of pseudonym certificates to the car via the LOP obscuring identification details.

Certificate Revocation

Any car or roadside device may report misbehaviour to the Misbehaviour Authority (MA) who is responsible for overseeing the certificate revocation process. The certificate revocation process is similar to the certificate provisioning process in reverse. The reporting device has to simply send the pseudonym certificate belonging to the offending device to the MA through a LOP. The MA requests initial keying materials from the PCA. The MA then sends the certificate request hash to the RA so that it can be added to the revocation blacklist. The MA also sends the keying material to the two Linkage Authorities so that it can request the linkage seed for the current time period. The

linkage seed allows the system to detect and reject all future pseudonym certificates related to a particular certificate-provisioning request. Due to the nature of hash chains the RA will not be able to find and reject pseudonym certificates used earlier than time period. The MA adds the keying materials as well as the time period in the Certificate Revocation List (CRL). The CRL is then distributed to all devices that may receive pseudonym certificates.

Analysis

This section provides an informal analysis of the C-ITS PKI proposals with respect to the security requirements defined earlier.

Certification and Validation Issues

This section considers practical implementation issues with the EU and US cryptographic protocols and primitives that are used in the certification and validation of vehicle public keys.

Weaknesses in Cryptographic Primitives

Cryptographic algorithms and protocols are the building blocks of security and privacy on the Internet and are a core part of all C-ITS PKI proposals. Cryptographic algorithms are continually being improved as researchers break the security of old schemes or propose new more efficient schemes. Modern cryptographic protocols such as Secure Shell (SSH) and Secure Socket Layers (SSL) include a built in negotiation process to select common cryptographic algorithm. Protocols in the C-ITS PKI systems should be flexible enough to allow the negotiation of cryptographic protocols. Although this may leave things open for downgrading attacks.

Efficiency of Cryptographic Protocols

The EU standard does not use any special cryptographic protocols to reduce communication traffic. In comparison, the US standard proposal incorporates cryptographic mechanisms for ensuring the scalable generation of public key certificates. A relatively small amount of data is required when distributing the certificates in the US standard because of the butterfly key mechanism. However, the same amount of data is still required to be returned to the car when the PCA has generated the certificates. New cryptographic protocols can be designed to allow reduced communication protocols. Though this may require more trust and computation on board the car.

Privacy Issues

Privacy for certificate provisioning in the EU standard is provided by encrypting the signer ID of the LTC thereby obscuring the identity of the car from the PCA. To ensure that privacy is maintained against an adversary that monitors all traffic to and from the car, the car is required to store a number of pseudonym certificates (around 2000) at any one time. The car randomly selects certificates to use during communications. If the stored number of certificates is insufficient it will reuse them or request more certificates. There is a performance requirement in that the symmetric decryption key needs to be requested before the pseudonym certificate can be used.

The certificate provisioning process in the US standard is complicated because of the multiple entities involved and the fact that each of these entities must hide information from the other entities to ensure the privacy of the car and its pseudonyms. The blinding process involves cryptographic

mechanisms, but also there is a need to store messages for some time so that traffic communication cannot be analysed. This will impact on the efficiency of the provisioning process. It is not recommended that the RA stores these values as it can then start to collect information that may allow it to link pseudonym certificates together.

Revocation issues

The major issue with the EU standard key revocation process is that an adversary-controlled car can continue to send invalid messages until it runs out of pseudonym certificates. This may be some time as cars are expected to store up to 2000 certificates.

There are issues with the US standard key revocation process in that it is assumed that all misbehaviour reports are valid. However, if this is request is submitted through a LOP, bogus misbehaviour reports may be submitted without being able to determine who submitted them. Thus a malicious attacker may have a car incorrectly revoked from the system.

The more entries in the CRL means that more linkage seeds must be verified by messages receivers before they can trust and act on the message. A malicious attacker could slow the system by reporting many invalid pseudonym certificates thereby greatly increasing CRL entries.

The US standard does have a weakness in the revocation process. If a car strays out of CRL broadcast range, they may not be updated with the latest CRL. An attacker blocking the signal to the car and preventing it from receiving the CRL update will achieve the same result. Thus the car will accept revoked certificate because it does not know that it is on the CRL. A car can also be tricked into accepting an expired out of date certificate (certificates usually have an expiry date). If the clock in a car is changed or naturally too slow, the car may accept an expired certificate. Most cars should be able to synchronise their clocks from a GPS signal, but this signal can be spoofed or blocked. Attackers can also target the timing system if they know this is a specific vulnerability that will work.

Scalability and Efficiency Issues

Certificate Provisioning Issues

Both the EU and US standards of securing V2V communications relies on a centralised certificate authority model of trust similar to the Internet. The Internet PKI in 2010 had around 650 organisations distributed worldwide providing certificate provisioning (Eckersley & Burns, 2010). It is roughly estimated in August 2012 that there is anywhere between 2.5 to 4 million certificates in use, with the figure increasing every year (Duncan, 2015). The number of certificate revocations may provide an indication on the number of certificates being issued to replace the revoked certificates. Between January 2012 to June 2014, the SANS institute estimated that approximately 1.5 million certificates were revoked (Vandeven, 2014). Although this figure includes certificates, which have ceased operation, where no replacement certificate is generated, this data provides insight on the order of magnitude of certificate provisioning on the Internet.

In comparison to the Internet PKI model, the C-ITS PKI will have to provide a significantly larger amount of certificate provisioning. The US model alone will have to support 350 million cars at full implementation, with that number continually increasing. To provide privacy, each car will need 40 pseudonym certificates per week, equating to 14 billion certificates provisioned each week.

Assuming a best-case scenario of a uniform distribution of certificate provisioning over the course of the week, the C-ITS PKI would have to provision 23,000 pseudonym certificates per second. Given modern computing power, such a load is feasible. However, due to geography and driving patterns, some infrastructure may experience higher than normal loads, as certificate provisioning would occur in a non-uniform distribution. There is an order of magnitude difference in number of certificates to issue and revoke for the C-ITS PKI which highlights a scalability issue. Although the number of entities in Australia is considerably less than the US and EU, the number of certificates provisioned annually still significantly exceeds the number of certificates the Internet provisions. Even under this reduced load, certificate provisioning and revocation for an Australian V2V system highlights a scalability issue.

Table 1. Certificate Comparison between Internet and C-ITS PKI

	Internet	**V2V (US)**	**V2V (AU)**
Number of Entities	1 Billion +	350 Million +	18 Million +
Certificates Provisioned (Annually)	1 to 2 Million*	278 Billion	37.4 Billion
Certificates Provisioned (Weekly)	19,000 to 38,000^	14 Billion	720 Million
Certificates Provisioned (Per Second)	-	23,000^	1190^
CRL Number of Entries	136,000#	-	-
CRL File Size	5.0 Mb#	Estimated 300 bytes to 2Mb+	Estimated 300 bytes to 2Mb+

* Based on estimations of revocation and expiry dates of certificates. ^ Assuming uniform distribution. # As of July 2015

Certificate Revocation Issues

With certificate provisioning orders of magnitude greater in the V2V network when compared to the Internet, even for an Australian V2V system, certificate revocation will also pose a scalability challenge. Although the certificate revocation details in the US standard are still yet to be finalised, there are several important considerations.

The first is the size of the CRL file. With a large number of entities in the network, and more certificates provisioned in a week in the V2V network than over the Internet in a year, the CRL file size may become very large. Currently, the SANS institute uses the Global Sign CRL list (GlobalSign, 2015), which as of July 2015 contained approximately 136,000 serial numbers of revoked certificates totalling to a CRL file size of 5.0 Mb. These include certificates revoked over a 4-year period since June 2011. Assuming the conservative estimate of a V2V CRL file size to be 5 MB, under the DSRC WAVE protocol (Li, 2010), each car would require 1.5 to 13 seconds to receive the CRL. PKI implementations using CRLs for certificate revocation are communications heavy (Naor & Nissim, 2000). A more efficient method called Online Certificate Status Protocol (OCSP) reduces the communications overhead, however requires the car to poll a server to verify

the validity of a certificate. This may be infeasible in a large geographic expanse that a V2V network will cover.

The second consideration is the subject to a Denial of Service (DoS). CRLs typically have a short validity period to ensure freshness of data. When they expire, the entity will poll the CRL distributor for a new or fresh CRL to prevent a replay attack using an old CRL. However, if a new CRL cannot be obtained before the previous one expires, the entity will be subject to a DoS. The CRL in this instance provides the only method of determining the validity or authenticity of an unexpired certificate. As a result, operations involving that certificate, such as verifying the authenticity of a message signed by that certificate cannot take place.

A possible solution to both these considerations is to use Delta CRLs, where only the changes to a CRL are distributed. Disseminating only the differences would reduce the communications overhead, whilst regular updates when in communications range would provide freshness of data. As each car maintains their own CRL, replay attacks on older CRLs being distributed can be avoided provided that CRL entries in each car could not be deleted.

Discussion and Conclusion

There are still a number of challenges for deploying a secure and effective C-ITS PKI. Australia has a large geographic environment, with large distances between cities. This differs from the EU and US standard environments with more regular interspersed urban centres. The proposed EU and US schemes therefore assume regular communications with central authorities for certificate provisioning and revocation. The challenges in deploying a C-ITS PKI in Australia would have to address the potential disruptions in network connectivity between vehicles and a central authority. As with the US and EU, the use of a more distributed and decentralised PKI architecture may be more applicable to deploying a C-ITS PKI, particularly in Australia with our large geographic environment and multiple state government agencies. However a decentralised system will make large-scale accurate certificate revocation more challenging.

The EU and US standards use the concept of pseudonyms to provide privacy. Currently, license plates on vehicles behave like pseudonymous identifiers that can be at any time revoked by transport registration authorities. Australia should consider whether the need for privacy from the authority entities in the Australian C-ITS PKI is necessary. This privacy requirement adds most of the complexity to the C-ITS PKI standards. It may be that there is a need for identities to be revealed under certain conditions such as when a legal warrant is provided.

The Australian C-ITS PKI standard is still unknown but it should take lessons from the EU and US. Both standards deal with complex interactions with multiple authorities. Australia should limit the number of authorities with a uniform standard across the country and extended trusted communications between regional transport registration authorities. A simpler C-ITS PKI system design with less reliance on centralised authorities will ensure a successful implementation and cost effective operation.

References

Alzaid, H., Foo, E., & Nieto, J. G. (2008, January). Secure data aggregation in wireless sensor network: a survey. In Proceedings of the sixth Australasian conference on Information security-Volume 81 (pp. 93-105). Australian Computer Society, Inc..

Bissmeyer, N., Stubing, H., Schoch, E., Gotz, S., Stotz, J. P., & Lonc, B. (2011). A generic public key infrastructure for securing car-to-x communication. In 18th ITS World Congress.

Duncan, R. (2015, May 13). Counting SSL certificates [Web log post]. Retrieved July 5, 2015, from http://news.netcraft.com/archives/2015/05/13/counting-ssl-certificates.html

Eckersley, P., & Burns, J. (2010, July), An Observatory for the SSLiverse. Retrieved from https://www.eff.org/files/defconssliverse.pdf

GlobalSign. (2015, July 3). Certificate Revocation List. Retrieved from http://crl.globalsign.com/gs/gsorganizationvalg2.crl

Harding, J., Powell, G., R., Yoon, R., Fikentscher, J., Doyle, C., Sade, D., Lukuc, M., Simons, J., & Wang, J. (2014, August). Vehicle-to-vehicle communications: Readiness of V2V technology for application. (Report No. DOT HS 812 014). Washington, DC: National Highway Traffic Safety Administration.

Li, Y. (2010). An Overview of the DSRC/WAVE Technology. Retrieved from http://www.nicta.com.au/pub?doc=4390

Naor, M., & Nissim, K. (2000). Certificate revocation and certificate update. Selected Areas in Communications, IEEE Journal on, 18(4), 561-570.

Vandeven, S. (2014, July 15), Digital Certificate Revocation. Retrieved from https://www.sans.org/reading-room/whitepapers/certificates/digital-certificate-revocation-35292

Whyte, W., Weimerskirch, A., Kumar, V., & Hehn, T. (2013, December). A security credential management system for V2V communications. In Vehicular Networking Conference (VNC), 2013 IEEE (pp. 1-8). IEEE.