Secure Vehicle-to-Infrastructure Communication: Secure Roadside Stations, Key Management, and Crypto Agility

Markus Ullmann* †, Christian Wieschebrink*, Thomas Strubbe*, and Dennis Kügler*
* Federal Office for Information Security
D-53133 Bonn, Germany
Email: {markus.ullmann christian.wieschebrink thomas.strubbe dennis.kuegler}@bsi.bund.de
† University of Applied Sciences Bonn-Rhine-Sieg
Institute for Security Research
D-53757 Sankt Augustin, Germany
Email: markus.ullmann@h-brs.de

***Abstract*—With the rising interest in vehicular communication systems many proposals for secure vehicle-to-vehicle communication were made in recent years. Also, several standardization activities concerning the security and privacy measures in these communication systems were initiated in Europe and in US. Here, we discuss some limitations for secure vehicle-to-infrastructure communication in the existing standards of the European Telecommunications Standards Institute. Next, a vulnerability analysis for roadside stations on one side and security and privacy requirements for roadside stations on the other side are given. Afterwards, a proposal for a multi-domain public key architecture for intelligent transport systems, which considers the necessities of road infrastructure authorities and vehicle manufacturers, is introduced. The domains of the public key infrastructure are cryptographically linked based on local trust lists. In addition, a crypto agility concept is suggested, which takes adaptation of key length and cryptographic algorithms during PKI operation into account.**

***Keywords*–Vehicular Ad hoc Networks; Vehicle-to-Vehicle Communication; Vehicle-to-Infrastructure Communication; Intelligent Transport System; Public Key Infrastructure**

I. Introduction

Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure communication (V2I) (consolidated V2X) has been discussed intensively in recent years. To specify use cases and prepare the necessary standardizations for the V2X communication, the Car2Car Communication Consortium was initiated by European vehicle manufacturers, equipment suppliers, research organisations and other partners.

The wireless communication technology for cooperative V2X communication is based on the IEEE 802.11p standard. A frequency spectrum in the 5.9 GHz range has been allocated on a harmonized basis in Europe in line with similar allocations in US. The neccessary specification and standardization in Europe is done by the European Telecommunications Standards Institute (ETSI). This includes the security standardization as well.

The ETSI standards for intelligent transport systems (ITS) specify a basis set of applications, like emergency vehicle warning, traffic light optimal speed advisory or co-operative local services (e.g., automatic access control and parking management). Different types of messages are defined for information exchange to support these use cases (see Section III). According the ETSI specifications messages shall be digitally signed by the sender (vehicles or roadside stations) to guarantee message integrity and authenticity. In order to issue and authenticate the corresponding cryptographic keys a suitable public key infrastructure (PKI) has to be established.

A first analysis of the current ETSI specifications and a proposal for a PKI, which regards the needs of infrastructure authorities and vehicle manufacturer was given in [1].

The first milestone in applying this technology in a realistic setting was the SimTD project with more than 100 vehicles equipped with V2V communication technology in the Frankfurt area in Germany in 2012 and 2013, see [2]. In a next step, the V2X technology will be deployed in large scale intelligent mobility infrastructure projects, for example, SCOOP@F [3] in France and the C-ITS corridor Rotterdam-Frankfurt-Vienna [4]. The main objective of the C-ITS corridor project is to increase road safety and provide the basis for an improved traffic flow.

In the C-ITS project roads work warning trailers are equipped with a digital gateway (RWWG) to communicate with the bypassing vehicles.

Two services are planned in the C-ITS corridor project:

- Send warning information via the road works warning gateway to the vehicles within the radio range. This message can be displayed in the infotainment device of the vehicle to inform the driver about the existing road works. So, the driver will be informed about the existing road works much earlier than today.
- Collect short range messages of bypassing vehicles by the RWWG to establish a traffic situation overview.

The purpose of the SCOOP@F project is to enhance the road safety and the travel quality. Therefore, five tests sites are established (e.g., Paris-Strasbourg highway, Bordeaux and its by-pass road) to examine V2X communication and to evaluate new services. In this project 3000 vehicles and 2000 km of streets will be equipped with ITS communication technology. This communication infrastructure facilitates the communication between vehicles and roadside stations to exchange

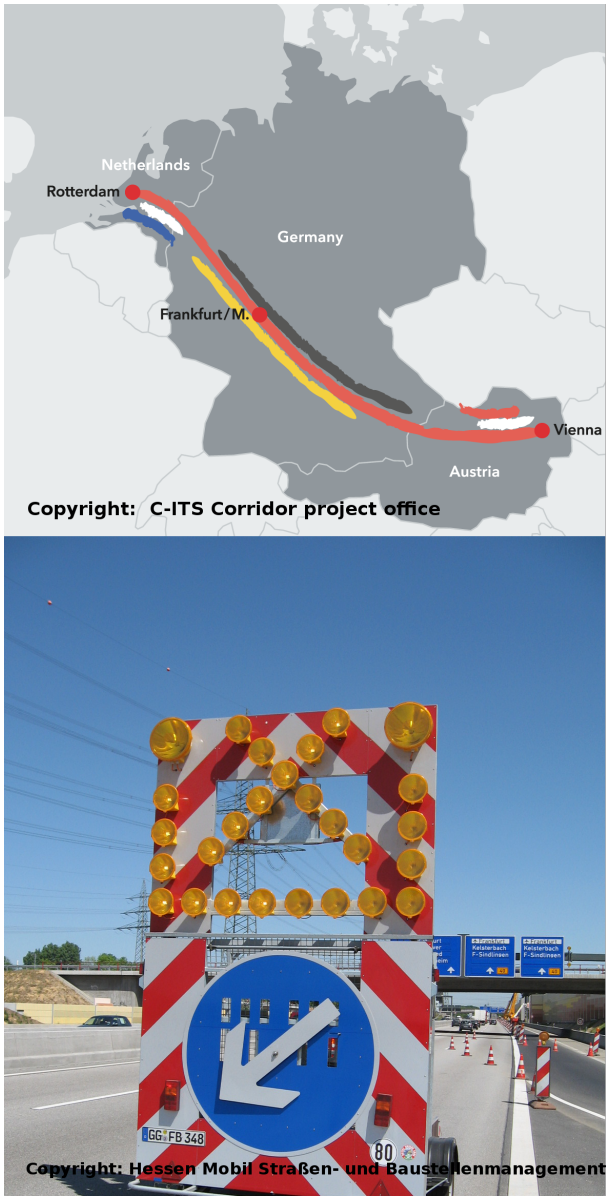

Figure 1. Road works warning trailer with digital road works warning gateway to communicate with the bypassing vehicles within the motorway C-ITS corridor Rotterdam-Frankfurt-Vienna

information. Vehicles communicate their geographic position, speed, obstacles, etc. while ITS roadside stations broadcast information concerning traffic conditions, works, speed limit, etc.

These projects mark only the very beginning of ITS technology deployment in Europe. Further plans like the integration of V2X gateways in roadside emergency telephones, sign gantries, etc. are already made.

The establishment of exhaustive V2X communication requires that existing physical infrastructure components (road works warning, road signs, lights, emergy telephones, etc.) are replaced by digitalized versions or upgraded with ITS communication gateways. However, ITS roadside stations (IRS) are often located in untrusted environments. If no effective security measures are taken physical manipulation of IRS in order to distribute false messages is easy. Therefore, the question arises which attacks are conceivable and which security measures has to be chosen so that vehicles can trust messages originating from ITS roadside stations. The importance of trust in V2X messages of ITS roadside stations will increase over time especially if automated vehicles will use the electronic information for vehicle control (e.g., adapt vehicle speed according to traffic light state).

In this paper, we regard the secure V2X communication especially from an infrastructure perspective. We identify measures that are needed so that a vehicle can trust V2X messages sent by ITS roadside stations. Therefore, we present results of a risk analysis for ITS roadside stations and derive security requirements. The security requirements adress the architecture of an IRS as well as the key management. Due to the specified usage of asymmetric cryptography (digital signature algorithms) a public key infrastructure is required. A number of practical considerations has to be taken into account when designing such a PKI.

- Many different stakeholders like vehicle manufacturers, transportation infrastructure authorities, etc. participate in ITS, especially in multi-national (e.g., European) systems. The PKI should provide flexibility to support different operators managing the vehicles and ITS roadside stations in their respective responsibilities.
- Requirements on cryptographic algorithms, domain parameters, key lengths, etc. may change over time due to new weaknesses and attacks or the increase of computer performance. In general, this means that a PKI needs a crypto agility concept to switch to a new cryptographic setting during its (possibly long) lifetime.
- Revocation of certificates and distribution of certificate revocation lists in time to all entities may turn out to be challenging in complex ITS scenarios. A simple alternative should be used to avoid distribution of certificate revocation lists.

Moreover, we introduce a multi-domain PKI for intelligent transport systems based on Local Trust Lists (LTL). This concept considers a PKI domain for vehicles (ITS vehicle stations) and different PKI domains for infrastructure components (ITS roadside stations). A PKI domain for ITS roadside stations is slightly different from the PKI concept proposed by [5]. Our approach guarantees that the infrastructure components remain under control of the particular infrastructure authority. In the ITS literature certification authorities are termed very different. Due to ongoing and trend-setting work of the security working group of the C-ITS platform we will use the naming conventions of this group. Certification authorities, which issue long term valid certificates are termed Enrolement Authority (EA). Certification authorities, which issue credential - or pseudonymous certificates are termed Authorization Authority (AA).

The PKI for ITS roadside stations (IRS PKI) is interoperable with the PKI for vehicles (IVS PKI). The IRS PKI for ITS roadside stations consists of two parts: an Enrolement Authority (EA) for issuing certificates for the identification of IRS gateways and an Authorization Authority (AA) for issuing authorization certificates to IRS gateways. With the

AA we take the hostile environment of IRS gateways into account. Although a PKI alone can not prevent local attacks on ITS roadside stations, it can mitigate their effects to a certain degree.

Our PKI proposal for ITS roadside stations supports cryptographic agility in the sense that modifications of cryptographic keys and algorithms during lifetime of the PKI are possible.

Finally, we derive necessary modifications of the existing ETSI certificate format [6] to be compatible to our concept because mechanisms for the delegation of rights and a crypto agility approach are missing to date. Here, we address only modifications to the ETSI certificate format, which are motivated from an infrastructure perspective.

The following sections are organized as follows: Section II is a description of related work. Section III provides a brief overview of the secure V2V communication specified in the according ETSI standards. Also, the suggested PKI architecture for ITS vehicle stations (IVS PKI), specified in [5], is described. Here, we state the problems if this IVS PKI is used for issuing certificates for IRS gateways, too. Security and privacy requirements for ITS roadside stations are given in Section IV. In the next Section V, the multi-domain PKI approach, the PKI concept for IRS gateways and the crypto agility proposal are introduced. Finally, in Section VI we summarize our results.

II. Related Work

Security and privacy issues in vehicular ad-hoc networks (VANETs) are addressed in many research papers. A detailed overview of attacks in VANETs is given by Ghassan Samara et al. in [7]. A security and privacy architecture for pseudonymous message signing is described in [8]. Here, a public key infrastructure is regarded, too. In [9], Julien Freudiger et al. suggested mix zones for location privacy in vehicular networks. Giorgio Calandriello et al. propose on-board, on-the-fly pseudonym certificate generation and self-certification. The authors developed this approach to alleviate one of the most significant limitations of the pseudonym-based approach: the need for complex management. To achieve this, the use of group signatures is proposed. Panagiotis Papadimitratos reports the research status of secure vehicular communication in the year 2008 [10]. Ma Di and Gene Tsusik give an overview about security and privacy in emerging wireless networks including VANETs [11]. Overall, a good overview concerning security and privacy in V2X communication can be found in [12].

More technical research results are archieved in public co-founded research projects. Here, we mention EVIVA [13] and OVERSEE [14], both co-founded by the european union. EVIVA addresses secure in-vehicle communication whereas the main objectives of the OVERSEE platform are techniques for strong isolation between independent applications to ensure that vehicle functionality and safety cannot be harmed by any other application.

A detailed analysis of privacy requirements and a comparison with the security requirements in VANETs is given in [15]. Further security and privacy concepts are presented in [16], [17], [18], [19], and [20]. Wiedersheim et al. [21] analyzed the location privacy in a specific communication scenario. Vehicles send beacon messages periodically. The beacons only carry the geographic position and an identifier. To support location privacy, the vehicles use pseudonymous identifier that are changed regularly. Assuming a passive attacker who is able to eavesdrop the communication in a specific region the attacker is able to track the vehicles with an accuracy of almost 100% if he uses the approach in [21].

A first analysis of vehicular data in cooperative awareness messages (CAM) and dezentralized environmental notification messages (DENM) messages like geographic position, speed, etc. from a data protection perspective is given in [22]. In this report CAM and DENM messages are regarded as *personal data*.

Different trust models for multi-domain PKIs on a generic level are described in [23], [24]. Here, we will follow the naming convention of [24]. It distinguishes between end entities (EE), that are subject of a certificate, Certification Authorities (CAs), that issue certificates, and root CAs, which are on top of a hierarchy of CAs. In [5] Norbert Bissmeyer et al. suggest a PKI for securing V2X communication. The Car2Car communication consortium adopted this proposal. We outline this IVS PKI in the following section.

III. Brief Overview on Secure V2X Communication

A. Communication

First, the ETSI specifications define a basic set of applications for ITS, like

- Active road safety (e.g., emergency vehicle warning, slow vehicle indication),
- Co-operative traffic effiency (e.g., regular speed, limits notification),
- Co-operative local services (e.g., automatic access control and parking management), and
- Global internet services (e.g., fleet management, loading zone management).

ITS applications are distributed among ITS stations that can be equipped with multiple communication capabilities. To date for V2X only broadcast communication based on IEEE 802.11p is provided. So, V2X is a short range communication technology with a communication range of about 600 m in open space.

The ETSI ITS architecture [25] distinguishes 4 different ITS roles termed ITS station types:

- ITS roadside stations, typically termed road side unit (RSU),
- ITS vehicle stations,
- ITS central stations, e.g., traffic operator or service provider, and
- ITS personal stations, e.g., a handheld device of a cyclist or pedestrian such as a smart phone.

The ITS stations exchange information mainly based on two different specified message types:

- Cooperative Awareness Message (CAM), and
- Dezentralized Environmental Notification Message (DENM).

CAMs are comparable with beacon messages. They are broadcasted periodically with a packet generation rate of 1 to

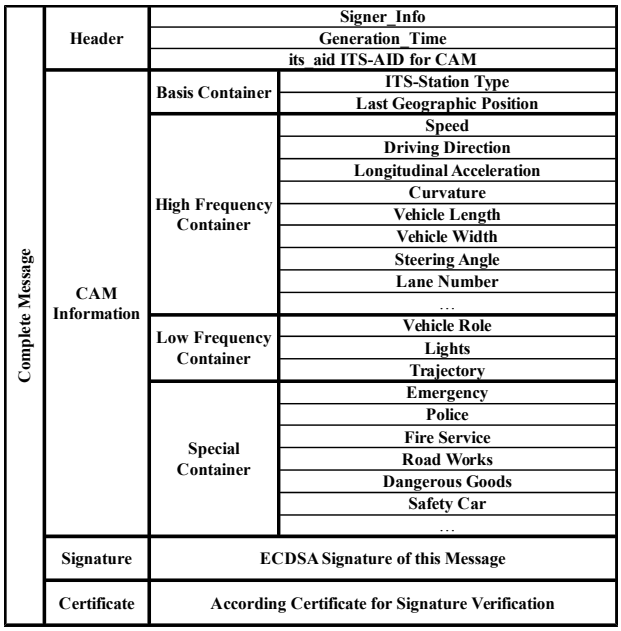

Figure 2. Examplary message format of a CAM. The CAM consists of a header, different data containers, e.g., the basis container, a signature and the appropriate certificate

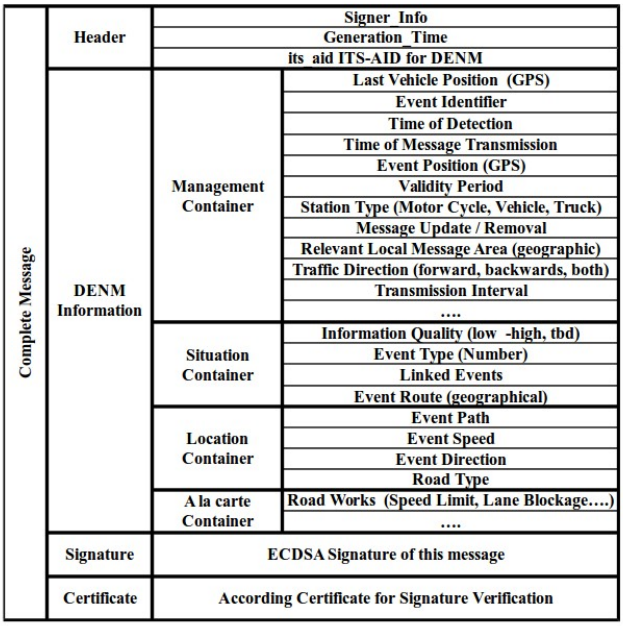

Figure 3. Examplary message format of a DENM. The DENM consists of a header, different data containers, e.g., the management container, a signature and the appropriate certificate.

10 Hz. Based on received CAM messages, ITS vehicle stations can calculate a local dynamic traffic map of their environment. It is not planned to forward CAM messages hop-to-hop. Figure 2 illustrates the structure of a CAM. The CAM is specified in detail in [26].

In contrast, the second message type, DENM, is event-driven and indicate a specific safety situation, e.g., road works warning (from an ITS roadside station) or a damaged vehicle warning (from an ITS vehicle station). The DENM message format is specified in detail in [27]. DENM messages can be transmitted hop-by-hop. RWWGs in the C-ITS project transmit DENM messages. Figure 3 illustrates the structure of a DENM.

B. Security and Privacy Architecture for Secure V2V Communication

1) ***Security****:* The designed security architecture [5] fulfills following security requirements:

1) Entity authentication: For entity authentication, each vehicular gateway has to be equipped with a *long term valid key pair* (secret key and corresponding public key E_{PK}) and a corresponding *long term valid certificate* E_{cert}. The key pair is generated at the gateway and the long term valid certificate E_{cert} is issued to a vehicle by the so called Enrolement Authority (EA) at the beginning of the vehicle's lifetime. The EA is part of the PKI described below. For the signatures ECDSA based on the NIST P-256 elliptic curve is applied. Certificates have to be structured according the defined ETSI format, see [6]. The validity period of a E_{cert} is not specified to date. That is to be specified within the common ITS PKI policy, which is in progress. Its final version is planned for publication in autumn 2016.
2) Message integrity and authentication: To realize message integrity and authentication the CAMs and DENMs are digitally signed using ECDSA, see Figures 2 and 3.
3) Message freshness and location protection: Assuming that ITS stations know their genuine geographic position and genuine current time they can detect replayed messages, because the geographic position and the transmission time are part of CAMs and DENMs.

Long term certificates and pseudonymous certificates are implemented based on the ETSI certificate format [6]. This certificate format was designed for the automotive domain and is still not widely applied yet. Primary design principle is shortness of the certificate format due to the necessary transmission over the wireless IEEE 802.11p channel.

2) ***Privacy****:* CAMs and DENMs should not reveal the identity of the vehicle (sender anonymity). Furthermore, it should not be possible to link messages of a vehicle (message unlinkability) over a longer period of time. Both requirements shall be sufficient to assure location privacy of the vehicle and his driver. Due to these privacy requirements, CAMs and DENMs are signed using pseudonymous certificates, which are not linked to an ITS vehicle station. Moreover, the used key and the according certificates are changed periodically. Therefore, an ITS vehicle station needs a set of pseudonymous certificates valid for some period of time. The set size and the pseudonym change frequency are not specified in [5] and will also be specified within the common ITS PKI policy.

An Authorization Authority (AA) is responsible for the

issuing of pseudonymous certificates $(A_{cert_1}, \ldots, A_{cert_N})$ to the vehicles. Pseudonymous certificates will only be issued to authenticated vehicles.

AA and EA operate under a root CA called ITS vehicle station root CA (IVS-RCA). To date, following revocation operations are provided: revocation of an EA and AA authorization certificate and revocation of vehicular long term certificates E_{cert}. The architecture of the IVS PKI domain is shown in Figure 4.

3) ***Shortcomings of this approach****:* As mentioned above the ETSI certificate format provides only elliptic curve cryptography based on the NIST prime curve P-256, [28]. No mechanism is provided to securely adapt key length or ECC domain parameter or cryptographic algorithms if necessary. In the meantime, the US National Security Agency (NSA) does not recommend to use this elliptic curve any more, [29].

Unfortunately, no detailed argumentation on this issue, only a hint of needed quantum resistant algorithms in a not too distant future, is given by NSA. N. Koblitz and A. Menezes attempt an evaluation of the various theories, speculations, and interpretations that have been proposed for this sudden change of course by the NSA [30].

The discussion shows that a crypto agility concept also for V2X communication is required.

In the final report of the C-ITS platform of the European Commission the data elements of CAM and DENM messages are rated as *personal data*, see [22]. This means, each vehicle broadcasts periodically with its CAMs digitally signed private data. Shortly spoken, each vehicle leaves a signed location trace. Every entity within the communication range can receive the data.

From our point of view, the pseudonym concept does not solve the vehicular privacy requirements. However, a detailed description of the V2V privacy problem is outside of the scope of this paper.

C. Using the IVS PKI for IRS Roadside Stations

The IVS PKI domain shown in Figure 4 has been proposed for issuing certificates to IRS gateways as well [5]. However, security and privacy requirements for vehicles and infrastructure components are not necessarily identical. In contrast to ITS vehicle stations, ITS roadside stations (road works warning, traffic lights, etc.) do not involve persons during operation comparable to a motorist. Usually, they operate without any human supervision. That is the reason that from our point of view, IRS gateways do not have to regard any privacy concerns. More details are given to this issue in Section IV-C. As consequence, IRS gateways do not really need a set of valid pseudonymous certificates at each time as it is designed for vehicles. Instead, we propose that IRS gateways need only one *Authorization Certificate* with a specific subject name identifying the IRS for each time frame. Due to the security considerations for IRS gateways, see Section IV-B, the validity period of authorization certificates for ITS roadside stations should be rather short. This means the requirements for certificates for vehicles and roadside stations are different.

Moreover, arising security weaknesses of the used security technology may be asessed differently by vehicle manufacturers on one side and infrastructure authorities on the other side. However, the rules of operation for a PKI domain are defined

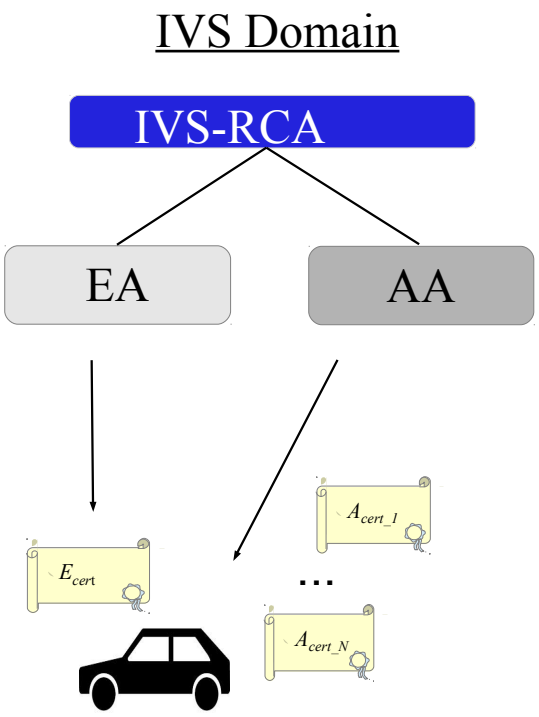

Figure 4. IVS PKI architecture promoted by the car2car communication consortium for ITS vehicle stations. This PKI consists of the Root Certification Authority (IVS-RCA), the Enrolement Authority (EA) and the Authorization Authority (AA)

in a single PKI policy, which will be specified by the root certification authority. For this reason, we propose a multi-domain PKI architecture: individual ITS PKIs under control of infrastructure autorities and an IVS PKI under control of the vehicle manufacturers, which are cryptographically linked to each other based on local trust lists (LTLs). The purpose of local trust lists is described in Section V-D.

So, each individual PKI domain can specify its own PKI policy for their specific needs. In addition, this multi-domain PKI architecture ensures that IRS unit gateways remain under control of the particular infrastructure authority. The idea of the common ITS PKI policy in progress in the security working group of the C-ITS platform of the EC DG MOVE is that individual PKI requirements can be specified in *Certificate Practise Statements*.

The concept of a multi-domain PKI architecture without any superior root CA is not new and already mentioned in [24]. It has been applied globally for electronic passports for many years. Here, each country operates its own root certification authority and has its own local trust list. The different national root certification authorities are cryptographically linked based on local trust lists. This concept works quite well and seems to be a good architecture approach for intelligent transport systems, too. The benefit of this approach is the possibility to configure PKI domains as needed. A drawback of the multi-domain PKI concept based on local trust lists is that each

PKI domain has to securely mange is own LTL. More details concerning this issue can be found in Section V-C.

IV. Security - and Privacy Requirements for ITS Roadside Stations

A. Vulnerability Analysis

In this section, we give a brief vulnerability analysis and formulate some security requirements for ITS roadside stations. When analysing possible threats to an IRS the operational environment has to be taken into account. Different types of ITS roadside stations operate in different environments with different degrees of trustworthiness. For example, one may assume that when a roadworks warning gateway is deployed at a construction site it is more or less under constant supervision of the (trustworthy) roadworks personnel. On the other hand, an IRS attached to traffic lights may be located in an unsupervised environment. In consequence, a traffic lights IRS may be subject to stronger attacks like hardware manipulation and thereby must match stronger security requirements. In the following, we take the conservative viewpoint and consider a hostile environment.

In [31], several threats towards vehicles and ITS roadside stations are analysed and corresponding (abstract) countermeasures are proposed. Summarizing the most important points of [31] (and somewhat extending the analysis), starting from the generic security goals availability, authenticity, integrity and confidentiality the following threats targeted at ITS roadside stations can be identified. The security goals may refer to incoming or outgoing messages.

- Threats to availability
  - jamming,
  - injection of a large number of forged or replayed messages.
- Threats to authenticity
  - masquerading (for example, as an legitimate IRS),
  - injection of forged messages or other data.
- Threats to integrity
  - injection of forged messages or other data,
  - altering of messages previously sent by vehicles,
  - replay of messages,
  - spoofing of GNSS information (or other sensor data),
  - spoofing time information.
- Threats to confidentiality
  - extraction of sensitive information (for example, cryptographic keys or other management data).

Attacks can either be facilitated locally or remotely. For example, forged messages can be either be transmitted via the wireless interface or they can be injected via some hardware interface at the IRS. Depending on the operational environment of the IRS both attack locations have to be accounted for.

In the setting of ITS applications the data sent out by an IRS is generally not considered confidential since it is intended to be used by any traffic participant. (As seen above from the perspective of data protection however the identity of vehicles or at least motorist is considered sensitive information.) On the other hand some cryptographic key material like signature keys stored on an IRS must remain confidential.

When implementing cryptographic mechanisms, these have to protected themselves in particular when considering a local attacker. For example, the keys for signing outgoing messages have to be stored in such a manner that they cannot be extracted since otherwise it can used by an attacker to masquerade as a legitimate IRS and to forge outgoing messages. Furthermore, it should not be possible to circumvent integrity and authenticity checks on an IRS.

More generally, an important factor to ensure the above security requirements is correct implementation. It should not be possible to introduce false traffic data or extract secret keys by exploiting weaknesses in the software (including the operating system) or hardware. In particular, it has to prevented that malicious software is installed on an IRS (for example, by an unprotected update procedure).

Cryptographic mechanisms themselves can be abused to facilitate denial of service attacks. For example, digital signatures require considerable computational effort for verification. An attacker (without the signing key) could produce and send out a large number of correctly formatted messages containing incorrect signatures. While checking these signatures the IRS may be unable to verify messages from legitimate senders.

As shown in [32], with some effort it is possible to simulate the signal of a Global Navigation Satellite System (GNSS) such that a wrong location is determined. This threatens the integrity of the data transmitted by an IRS. A wrong location of a roadworks site may be announced for example. It the GNSS signal is used to adjust the internal clock wrong time information may also be introduced. This can be possibly used by an attacker to mount replay attacks where old (already sent) messages are then accepted by the IRS.

B. Security Requirements

In addition to the security requirements in Section III-B the following security requirements are derived from the above vulnerability analysis.

- Since IRS possibly are located in hostile environments they should be equipped only with time restricted authorization to limit the timeframe for possible misuse.
- In order to protect secret key material the use of a secure hardware element is proposed. This secure element is hardened against side-channel and invasive attacks so that key extraction becomes very difficult. Secret key material is generated on this device.
- Only authentic and integrity protected (i.e., signed) software or firmware updates shall be accepted by the IRS.

Of course the connection of the IRS to the back-end system also has to be protected in particular regarding authenticity and integrity.

Attacks on the availability can be mitigated to some extent by non-cryptographic means. For example, jamming can be impeded by spread spectrum techniques like frequency hopping [33]. In order to mitigate attacks exploiting the computational overhead of cryptographics mechanisms fast

implementations in particular of the signature verification algorithm are required.

To counter GNSS attacks on ITS roadside stations the geographic location of IRS with a fixed geographic location should be statically coded. Also, for time synchronization a secure alternative to GNSS time synchronization should be used.

The analysis given here should only be considered as a starting point for more detailed security assessments for different types of ITS roadside stations. Security requirements for IRS gateways should be carefully specified in depth, e.g., in form of a Protection Profile (PP) according to Common Criteria.

If IRS gateways are verifiably resistant to active attacks they can play an import role as separate trust anchors in a cooperative ITS system, e.g., for implementing secure time synchronization, distribution of CRLs, etc.

C. Privacy Requirements

Current vehicles are controlled by the driver. Due to this issue, privacy concerns have to be regarded by the vehicular broadcast communication. In contrast to vehicles, ITS roadside stations are not directly controlled by a user. They operate without any direct personal reference. So, during the sending of messages of an IRS no personal data is revealed. Therefore, no privacy requirements are needed.

But if ITS roadside stations receive and process vehicular CAMs and DENMs privacy requirements may have to be fulfilled because vehicular CAMs and DENMs are regarded as personal data, see [22].

The main privacy requirement is to erase the personal reference of the data on the ITS roadside station immediately after the reception of it. If some use cases have to transmit data from ITS roadside stations to traffic control center, only anonymized data should be send, e.g., realized by data aggregation. Following this main requirement, we can isolate the privacy problem on ITS roadside stations and do not regard backend systems as well. If some use cases require the storage of CAM respective DENM messages on an IRS, e.g., to calculate a traffic situation overview, the stored data should be erased immediately after the processing of the data.

V. IRS PKI Concept

A. Role of Authorization Certificates for ITS Roadside Stations

The primary use case for IRS gateways is the transmission of local traffic information. Due to integrity and authenticity reasons, these messages have to be signed. Therefore, the IRS gateways need signature keys and according certificates. ITS roadside stations do not have to regard any privacy concerns, as explained in Section IV-C. Technically, this means that IRS gateways do not have to have pseudonymous keys and certificates. Instead, we propose that IRS gateways have only one valid authorization key pair and one corresponding authorization certificate at a time. Only in the transition phase between two certificate validity periods an IRS gateway two valid authorization certificates $C_{cert_{N-1}}$ and C_{cert_N} may be necessary.

The IRS gateway should be implemented in such a way that it acts in his designated role and transmits DENM messages only if it owns a valid authorization certificate. By this a possible misuse of IRS gateways is made more difficult.

B. IRS PKI Architecture

As mentioned above, we propose that ITS roadside stations have only one authorization key pair and one corresponding authorization certificate A_{cert} at each time. The secret key corresponding to such a A_{cert} is used for signing outgoing messages, e.g., DENM messages. For this reason, these certificates have to be implemented according to the ETSI certificate format. Since it is technically challenging to distribute certificate revocation lists (CRLs) to vehicles in time, authorization certificates should have a short validity period, for example, one day. Thereby implicit revocation of A_{cert} becomes possible by not issuing new authorization certificates to IRS gateways. The exact validity period of authorization certificates have to be specified according to a detailed risk assessment concerning the addressed IRS type. For example, RWWG are deployed for road works sites, which are usually established for one or two days. It may be good practice then to issue an authorization certificate with a maximal validity period of two days to a RWWG shortly before it is deployed.

For authentication purposes, e.g., to obtain authorization certificates (for example, on a daily basis) an infrastructure component requires a long term identification certificate E_{cert}. These long term certificates E_{cert} are issued by an Enrolement Authority (EA) during the enrolment of the IRS gateway. A long term certificate E_{cert} is used within a certificate request for authorization certificates towards the AA. We suggest that the authorization key pair is generated within the secure element of the IRS gateway and the authorization certificate is only issued after mutual authentication of IRS gateway and AA and only if the E_{cert} of the IRS gateway is not revoked. Therefore, the EA has to maintain a CRL for revoked long term certificates E_{cert}.

A long term identification certificate E_{cert} is only visible inside the IRS PKI and is not transmitted to vehicles. In particular, it is not communicated over the IEEE 802.11p channel. For this reason, we suggest to implement the long term identification certificates E_{cert} of ITS roadside stations according to the X.509 v3 certificate profile. This profile is widely applied and provides all necessary certificate services like time stamping, issuing CRLs, etc. The validity period of a E_{cert} should be at the order of years, e.g., five to six years for IRS gateways like RWWGs. A timeframe of five to six years seems to be reasonable considering progress in cryptanalysis or hardware security vulnerabilities. Due to different certificate issuing policies and certificate formats the EAs and the AAs are attached to different root certification authorities, which are called E-RCA and A-RCA respectively here, see Figure 5.

Due to the long validity periods of long term certificates, certificate revocation, implemented as a CRL according to X.509 v3, is suggested. Once a long term certificate is revoked, no authorization certificates are issued to the IRS gateway any more.

Due to the short validity period of authorization certificates of IRS gateways, the IRS gateways require an online communication channel, e.g., via GSM, LTE, etc. to receive new authorization certificates.

C. Crypto Agility

Figure 6 shows how the validity periods of the certificates within the IRS PKI domain relate to each other. The validity

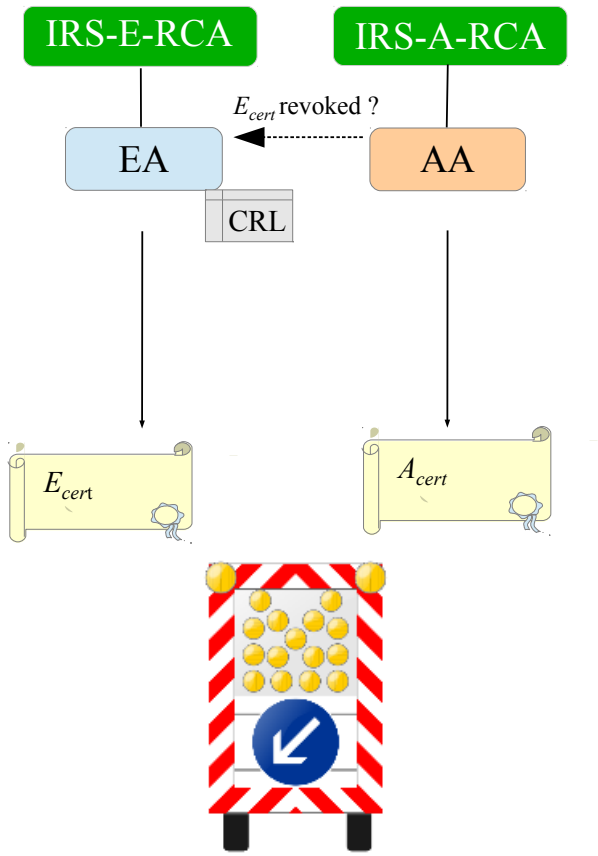

Figure 5. IRS PKI domain architecture. An IRS PKI domain consists of an EA for issuing long term certificates E_{cert} and an AA for issuing authorization certificates A_{cert}.

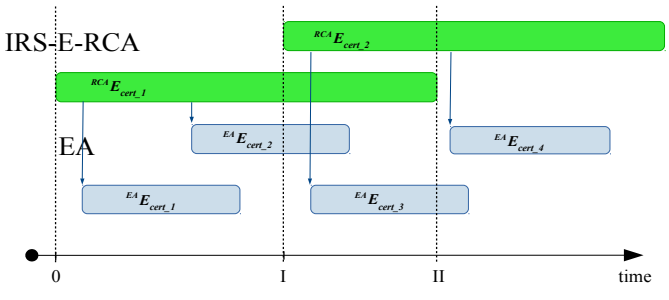

Figure 6. Certificate shell model. The validity period of a certificate is within the validity period of the issuing Certification Authority. E.g., the validity period of $^{EA}E_{cert\_1}$ is within the validity period of $^{RCA}E_{cert\_1}$

periods follow the shell model, i.e., the validity periods of certificates are enclosed in the validity periods of superior certificates.

1) A certificate of a certification authority (CA) is in one of three states: *active*, *passive* or *expired*. After generation of a key pair the according certificate is in state *active*. Over time the certificate state changes from *active* to *passive* to *expired*.
2) A certificate in state *active* is used for issuing certificates to subordinate CAs or IRS gateways.
   - Assume that an IRS-E-RCA root key pair (secret key: $^{RCA}E_{SK\_1}$, public key: $^{RCA}E_{PK\_1}$) is generated at time 0 of Figure 6. The secret key $^{RCA}E_{SK\_1}$ is used to sign and issue a self-certified E-RCA certificate $^{RCA}E_{cert\_1}$, first. The certificate $^{RCA}E_{cert\_1}$ is in state *active*.
   - The secret key $^{RCA}E_{SK\_1}$ is used to sign EA certificates: $^{EA}E_{cert\_1}$ and $^{EA}E_{cert\_2}$.
   - The certificate $^{RCA}E_{cert\_1}$ switches to state *passive* at time point *I* when the next root key pair (secret key: $^{RCA}E_{SK\_2}$, public key: $^{RCA}E_{PK\_2}$) and according certificate $^{RCA}E_{cert\_2}$ are issued. Now, the certificate $^{RCA}E_{cert\_2}$ is in state *active*. A certificate in state *passive* is not used to issue certificates any longer. However, it is still needed to verify already issued subordinate certificates. At time point *II* certificate $^{RCA}E_{cert\_1}$ expires.
3) Certificate $^{RCA}E_{cert\_2}$ is termed *Link Certificate* because it is signed with the former IRS-E-RCA secret key $^{RCA}E_{SK\_1}$.

Over long lifetimes the requirements for cryptographic mechanisms are changing. This has implications for the cryptographic mechanisms applied within the PKI domain, too. The cryptographic setting of the PKI has to be adapted according to current cryptographic requirements. All CAs in an ITS PKI have to follow the common PKI policy and the specific certificate practise statement of the root CA. Therefore, changes of a cryptographic setting for a whole IRS PKI are prescribed by the root certification authority E-RCA or A-RCA.

Changes to the following components due to newly discovered weaknesses are conceivable:

1) Elliptic curve domain parameters,
2) Hash algorithm,
3) Signature algorithm.

We suggest to implement a new PKI crypto setting by means of a link certificate, assuming that the certificate format allows the specification of cryptographic parameters. Obviously, modifications can only be applied if the infrastructure components are technically able to run the new algorithms.

The validity period of an E_{cert} and an A_{cert} differ a lot. An E_{cert} has a validity period of several years, whereas an A_{cert} has a validity period of few days at most. If the issuing certification authorities AA and IRS-A-RCA have similar short validity periods with respect to the shell model, the cryptographic settings between E_{cert} and A_{cert} can differ. In particular, shorter keys can be used for signing A_{cert}

towards signing an E_{cert}. Today, the ETSI certificate format only provides the NIST Elliptic Curve Domain Parameter P-256 with 256 bits long secret keys, see [28]. This key length is sufficient for the very near future but other ECC domain parameter should be used due to [29]. However, it is highly probable that longer key length have to be used for long term certificates E_{cert} in future.

D. Trust Establishment between PKI domains

An examplary architecture of a multi-domain PKI with three PKI domains (IRS_I, IVS and IRS_II) is shown in Figure 7. In our example there is only one IVS domain with the IVS-RCA to issue certificates for vehicles managed by the vehicle manufacturers and two separate IRS domains IRS_I and IRS_II with the root CAs A-RCA_I and A-RCA_II managed by different infrastructure authorities. These two IRS domains issue authorization certificates to IRS gateways in their respective domain. Now trust relations between the different PKI domains have to be established somehow. This can be accomplished by securely exchanging self-signed certificates of the respective root CAs of the PKI domains. Each root CA maintains a LTL containing the certificates of root CAs of other PKI domains it trusts. The LTL of a PKI domain is signed (for authentication reasons) and issued to all members of the domain by the root CA, e.g., A-RCA_I manages the LTL for the IRS_I domain. Each PKI domain can individually define the needed rules that are sufficient to trust a separate PKI domain.

To verify the authenticity of IRS gateway DENM messages in our examplary architecture, the vehicles have to know the root PKI certificates of the PKI domains IRS_I and IRS_II: ${}^{A-RCA\_I}A_{cert\_1}$ and ${}^{A-RCA\_II}A_{cert\_1}$. If the IVS PKI domain trusts in the IRS_I and IRS_II PKI domains the certificates ${}^{A-RCA\_I}A_{cert\_1}$ and ${}^{A-RCA\_II}A_{cert\_1}$ are elements of the LTL of the IVS PKI domain. Just after issuing of a new certificate, e.g., ${}^{A-RCA\_I}A_{cert\_2}$ for the infrastructure PKI domain IRS_I this certificate has to be appended to the LTL of the IVS PKI domain. Dependent on the validity period of the certificates ${}^{A-RCA\_I}A_{cert\_1}$ and ${}^{A-RCA\_I}A_{cert\_2}$ and due to the chosen shell model both certificates are valid for a defined time frame, see Figure 6. If a LTL of a PKI domain is changed all entities of the PKI domain (subordinate CAs and EEs) have to know this information. A time-critical situation arises when one specific PKI domain, e.g., the IRS_I PKI domain loses trust and has to be removed from the LTL of the IVS PKI domain. In this case all affected entities in the IVS PKI domain have to update their LTL as soon as possible.

Based on the currently discussed ITS applications, trust relations between the different ITS domains, here IRS_I and IRS_II, are not really required since no messages are exchanged between these domains. In our example the LTL of the two IRS domains just contain the current root certificate of the IVS PKI domain ${}^{RCA}E_{cert\_1}$.

E. Necessary ETSI Certificate Format Adaptations

In our paper, a multi-domain PKI based on LTLs and an according crypto agility concept is presented. The described mechanisms require some adaptation of the current ETSI certificate format.

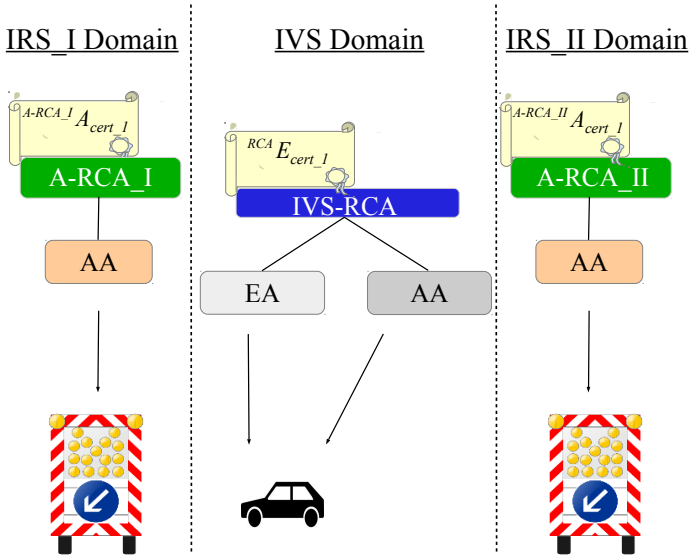

Figure 7. Examplary multi-domain PKI architecture with one IVS domain and two IRS domains: IRS_I and IRS_II.

a) Elliptic curve cryptography: The ETSI certificate format regards only Elliptic Curve Cryptography (ECC) performed on NIST domain parameters P-256. These domain parameters have a specific structure to perform ECC calculations very fast. But this structure opens specific side channel attacks. For example, even effective countermeasurements like point blinding and scalar blinding of ECC implementations are not sufficient to resist side channel attacks on NIST ECC implementations, see [34]. Therefore, further cryptographic ECC domain parameters (e.g., brainpool curves) should be added [35].

b) Rights management: Fire trucks and police vehicles need specific rights during action. These rights have to be coded within certificates, too. But only qualified CAs may issue these kind of certificates. The ETSI rights management concept should be enhanced in a sense that a subordinate CA can only assign restricted rights to issued certificates.

c) Link certificate: The ETSI certificate has to support link certificates to allow change of the root CA key and crypto agility as suggested in Section V-C.

VI. Conclusion

In this paper, a secure vehicle-to-infrastructure communication is discussed based on the existing ETSI standards. We constitute that the existing ETSI security specifications have some limitations. Especially, the missing crypto agility concept and adaptations on the ETSI certificate format are needed. Moreover, the proposed PKI of the Car2Car Communication Consortium for ITS vehicle stations (IVS PKI) does not regard all needs of ITS roadside stations. For this reason, we suggest a multi-domain PKI to adequately address the requirements of vehicle manufacturers and infrastructure authorities. The different PKI domains are cryptographically linked based on LTLs. In addition, a brief vulnerability analysis of ITS roadside stations is given.

As a next step, the IRS PKI architecture will be substantiated und implemented as a pilot system in the C-ITS corridor project to gather experiences. Beside that a common PKI policy is prepared within the security working group of the C-ITS platform of the EC DG MOVE for intelligent transportation systems in Europe. Important is that these common PKI policy enables specific requirement distinctions of PKI domains based on certificate practise statements to consider necessary differences between ITS vehicle stations and ITS roadside stations as shown in this paper.

VII. ACKNOWLEDGEMENT

The authors would like to thank Sandro Berndt and Arno Spinner from the Federal Highway Research Institute (BASt), our colleagues Nicolas Thenée and Hans-Peter Wagner and the anonymous referees for valuable remarks. Moreover, thanks to Hessen Mobile and the C-ITS Corridor project office for providing us with photo material.

REFERENCES

[1] M. Ullmann, C. Wieschebrink, and D. Kügler, "Public key infrastructure and crypto agility concept for intelligent transport systems," in Proceedings VEHICULAR 2015: The Fourth International Conference on Advances in Vehicular Systems, Technologies and Applications. IARIA, 2015, pp. 14–19.

[2] SimTD, "Secure intelligent mobility," 2008-2013, http://www.simtd.de/index.dhtml/deDE/index.html.

[3] European Commission, "SCOOP@F," 2013, http://inea.ec.europa.eu/en/ten-t.

[4] BMVI, "Cooperative its corridor rotterdam-franfurt-vienna joint deployment," 2014, http://www.bmvi.de.

[5] N. Bissmeyer, H. Stubing, E. Schoch, S. Gotz, J. P. Stotz, and B. Lonc, "A generic public key infrastructure for securing car-to-x communication," in 18th ITS World Congress, 2011.

[6] ETSI, "Intelligent Transport Systems (ITS);Security; Security header and certificate formats, ETSI TS 103 097 V1.2.1," 2015, http://www.etsi.org/.

[7] G. Samara, W. A. Al-Salihy, and R. Sures, "Security analysis of vehicular ad hoc nerworks (vanet)," in Network Applications Protocols and Services (NETAPPS), 2010 Second International Conference on. IEEE, 2010, pp. 55–60.

[8] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, "Architecture for secure and private vehicular communications," in Telecommunications, 2007. ITST'07. 7th International Conference on ITS. IEEE, 2007, pp. 1–6.

[9] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos et al., "Mix-zones for location privacy in vehicular networks," in Proceedings of the first international workshop on wireless networking for intelligent transportation systems (Win-ITS), 2007.

[10] P. Papadimitratos and J.-P. Hubaux, "Report on the secure vehicular communications: results and challenges ahead workshop," ACM SIGMOBILE Mobile Computing and Communications Review, vol. 12, no. 2, 2008, pp. 53–64.

[11] M. DI and G. Tsudik, "Security and privacy in emerging wireless networks," IEEE Wireless Communications, 2010, p. 13.

[12] Hagen Stübing, Multilayered Security and Privacy Protection in Car-to-X Networks - Solutions from Application down to Physical Layer. Springer Vieweg, 2013.

[13] E-safety Vehicle Intrusion proTection Applications, "Scientific publications," 2009-2011, http://www.evita-project.org/publications.html/.

[14] Open Vehicular Secure Platform, "Scientific publications," 2010-2012, https://www.oversee-project.com/.

[15] F. Schaub, Z. Ma, and F. Kargl, "Privacy requirements in vehicular communication systems," in Computational Science and Engineering, 2009. CSE'09. International Conference on, vol. 3. IEEE, 2009, pp. 139–145.

[16] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, vol. 15, no. 1, 2007, pp. 39–68.

[17] J. Camenisch, S. Hohenberger, and M. Ø. Pedersen, "Batch verification of short signatures," in Advances in Cryptology-EUROCRYPT 2007. Springer, 2007, pp. 246–263.

[18] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications," in INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, 2008.

[19] F. Armknecht, A. Festag, D. Westhoff, and K. Zeng, "Cross-layer privacy enhancement and non-repudiation in vehicular communication," in Communication in Distributed Systems (KiVS), 2007 ITG-GI Conference. VDE, 2007, pp. 1–12.

[20] K. Plößl and H. Federrath, "A privacy aware and efficient security infrastructure for vehicular ad hoc networks," Computer Standards & Interfaces, vol. 30, no. 6, 2008, pp. 390–397.

[21] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," in Wireless On-demand Network Systems and Services (WONS), 2010 Seventh International Conference on. IEEE, 2010, pp. 176–183.

[22] C-ITS Platform of the EC DG MOVE, "Final Report," 2016, http://ec.europa.eu/transport/themes/its/doc/c-its-platform-final-report-january-2016.pdf.

[23] J. Linn, "Trust models and management in public-key infrastructures," RSA laboratories, vol. 12, 2000.

[24] R. Nielsen, "Memorandum for multi-domain public key infrastructure interoperability, rfc 5217," Tech. Rep., 2008.

[25] ETSI, "ETSI EN 302 665 V1.1.1: Intelligent Transport Systems (ITS) - Communications Architecture," 2010, http://www.etsi.org/.

[26] ——, "ETSI EN 302 637-2 V1.3.2: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service," 2015, http://www.etsi.org/.

[27] ——, "ETSI TS 102 637-3 V1.2.1: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service," 2013, http://www.etsi.org/.

[28] Recommended Elliptic Curves For Federal Government Use, National Institute of Standards and Technology, July 1999. [Online]. Available: http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf

[29] National Security Agency, "Cryptography today," 2015, https://www.nsa.gov/ia/programs/suiteb_cryptography.

[30] N. Koblitz and A. Menezes, "A riddle wrapped in an enigma," Cryptology ePrint Archive, Report 2015/1018, 2015, http://eprint.iacr.org/.

[31] ETSI, "ETSI TR 102 893 V1.1.1: Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA). Technical Report," 2010, http://www.etsi.org/.

[32] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful gps spoofing attacks," in Proceedings of the 18th ACM conference on Computer and communications security. ACM, 2011, pp. 75–86.

[33] B. Sklar, Digital Communications, Second Edition. Prentice Hall PTR, 2001.

[34] B. Feix, M. Roussellet, and A. Venelli, "Side-channel analysis on blinded regular scalar multiplications," in Progress in Cryptology–INDOCRYPT 2014. Springer, 2014, pp. 3–20.

[35] Brainpool, "ECC Brainpool Standard Curves and Curve Generation, Version 1.0, available online at http://www.ecc-brainpool.org/ecc-standard.htm," 2005.