Public Key Infrastructure and Crypto Agility Concept for Intelligent Transportation Systems

Markus Ullmann* †, Christian Wieschebrink* and Dennis Kügler*
* Federal Office for Information Security
D-53133 Bonn, Germany
Email: {markus.ullmann christian.wieschebrink 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*—Secure vehicular communication has been discussed over a long period of time. Now,- this technology is implemented in different Intelligent Transportation System (ITS) projects in europe. In most of these projects a suitable Public Key Infrastructure (PKI) for a secure communication between involved entities in a Vehicular Ad hoc Network (VANET) is needed. A first proposal for a PKI architecture for Intelligent Vehicular Systems (IVS PKI) is given by the car2car communication consortium. This architecture however mainly deals with inter vehicular communication and is less focused on the needs of Road Side Units. Here, we propose a multi-domain PKI architecture for Intelligent Transportation Systems, which considers the necessities of road infrastructure authorities and vehicle manufacturers, today. The PKI domains 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 (VANETs), Vehicle-to-Vehicle Communication (V2V), Vehicle-to-Infrastructure Communication (V2I), Secure Intelligent Transport Systems, Public Key Infrastructures

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 all the necessary standardizations for V2V and V2I communication, the Car2Car Communication Consortium was initiated by European vehicle manufacturers and supported by equipment suppliers, research organisations and other partners [1]. The results of the technical discussions are a collection of ETSI (European Telecommunications Standard Institute) standards. 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 ITS corridor, a joint Intelligent Transportation System (C-ITS) cooperation between Austria, Germany and the Netherlands [4]. In the C-ITS project Roads Work Warning Trailers are equipped with a digital Road Works Warning Gateway (RWWG) to communicate with the bypassing vehicles. This projects mark only the very beginning of ITS technology deployment in Europe. Further plans are already mentioned: the integration of V2X gateways in roadside emergency telephones, sign gantries etc.

The wireless communication technology for cooperative V2V and V2X communication is based on the IEEE 802.11p standard. For this, 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 is sone by the ETSI. This includes the security standardization as well [5].

According to these standards messages transmitted by vehicles or RSUs shall be digitally signed to guarantee integrity and authenticity. In order to authenticate the corresponding keys a suitable PKI has to be established. 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 RSUs in their respective responsibilities.
- Requirements on cryptographic algorithms, domain parameters, key lengths etc. may change over time due to new weaknesses, new attacks or the increase of computer performance. In general, this means that a PKI needs a concept to switch to a new cryptographic setting during its (possibly long) lifetime.
- Revocation of certificates may turn out to be challenging in complex ITS scenarios. A simple mechanism for revoking signing rights should be used.

In this paper, we introduce a multi-domain PKI for ITS based on Local Trust Lists (LTL). This concept considers a IVS PKI domain and different ITS PKI domains. A ITS PKI domain is slightly different to the IVS PKI proposed by the Car2Car Communication Consortium [6]. First, our approach guarantees that the infrastructure components (Road Side Units (RSU)) remain under control of the particular infrastructure authority. Second, the ITS PKI is interoperable with the IVS PKI for the vehicles. This ITS PKI consists of two parts: a Long Term Certification Authority (LT-CA) for the identification of RSU gateways and a credential CA (C-CA) for issuing credential certificates to RSU gateways. With the C-CA we take the hostile environment of RSU gateways into account. We assume that attackers are able to manipulate the RSUs like roadside emergency telephone gateways, sign gantry gateways etc. physically. A PKI can not prevent such kind of attacks, but mitigate their effects to a certain degree.

Our ITS PKI proposal 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 [5] to be compatible to our concept because concepts 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. Within this paper we do not analyze the pseudonym concept in depth, which is proposed to assure sender anonymity and message unlinkability for vehicles. (We briefly present this concept in chapter III-B.)

The following sections of this paper 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 Intelligent Vehicle Systems, specified in [6], is described. Here, we state the problems if this IVS PKI is used for issuing certificates for ITS RSU gateways, too. In the next Section IV, the multi-domain PKI and ITS PKI concept for RSU gateways and the crypto agility proposal are introduced. Section V briefly addresses security requirements for RSU gateways. Finally, in Section VI we summarize our results.

II. Related Work

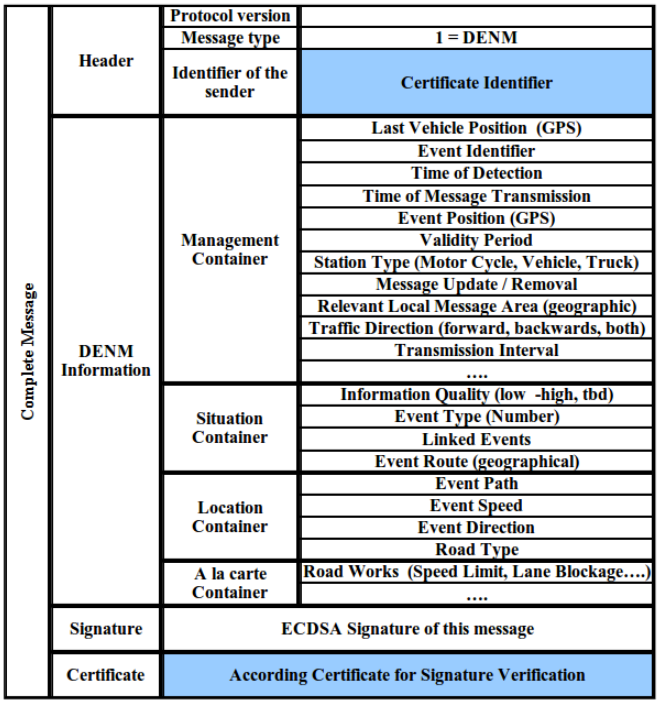
Security and privacy issues in Vehicular Ad hoc Networks (VANETs) are addressed in a lot of research papers. A detailed overview of attacks in VANETs is given by Ghassan Samara et al. in [7]. Di Ma and Gene Tsusik give an overview about security and privacy in emerging wireless networks including VANETs. Overall, a good overview concerning security and privacy in V2X communication can be found in [8]. A detailed analysis of privacy requirements and a comparison with the security requirements in VANETs is given in [9]. Beside that, further security and privacy concepts are presented [10], [11], [12], [13], and [14].

Different trust models for multi-domain PKIs are described in general in [15], [16]. Here, we will follow the naming convention of [16]. It distinguishes between End Entities (EE), that are subject of a certificate (vehicle or RSU gateway), Certification Authorities (CAs), that issue certificates, and root CAs, which are on top of a hierarchy of CAs. In [6] Norbert Bissmeyer et al. suggest a generic PKI for securing V2X communication. The car2car communication consortium adopted this proposal. We outline this IVS PKI in Section III.

III. Brief Overview Secure V2X Communication

A. Communication

In the ETSI ITS architecture [17] two different message types are defined. Cooperative Awareness Messages (CAMs) are broadcasted periodically with a maximum packet generation rate of 10 Hz. Based on received CAM messages, vehicles can calculate a local dynamic map of their environment. It is not planned to forward CAM messages hop-to-hop. In contrast, the second message type, Dezentralized Environmental Notification Messages (DENMs) , are event-driven and indicate a specific safety situation, e.g., road works warning (from a RSU gateway) or a damaged vehicle warning (from an IVS gateway). DENM messages can be transmitted hop-by-hop. RWWGs in the C-ITS project transmit DENM messages. Figure 1 illustrates the structure of the DENM message format. For road sign and traffic light gateways etc. new message formats have still to be specified in future.



Complete Message	Header	Protocol version	
		Message type	1 = DENM
		Identifier of the sender	Certificate Identifier
	DENM Information	Management Container	Last Vehicle Position (GPS)
			Event Identifier
			Time of Detection
			Time of Message Transmission
			Event Position (GPS)
			Validity Period
			Station Type (Motor Cycle, Vehicle, Truck)
			Message Update / Removal
			Relevant Local Message Area (geographic)
			Traffic Direction (forward, backwards, both)
			Transmission Interval
			….
		Situation Container	Information Quality (low -high, tbd)
			Event Type (Number)
			Linked Events
			Event Route (geographical)
		Location Container	Event Path
			Event Speed
			Event Direction
			Road Type
		A la carte Container	Road Works (Speed Limit, Lane Blockage….)
			….
	Signature	ECDSA Signature of this message	
	Certificate	According Certificate for Signature Verification	

Figure 1. Examplary message format of DENM. The DENM consists of a header, different data containers, e.g., the management container, a signature and the appropriate certificate.

B. Security and Privacy Architecture for Secure V2X Communication

To guarantee message integrity and authenticity, all CAM and DENM messages are signed with the cryptographic signature algorithm ECDSA by the sender. Due to privacy requirements (sender anonymity and message unlinkability), the messages are signed using pseudonymous certificates where the used keys and certificates are changed periodically. Therefore, a vehicular gateway has a set of N valid pseudonymous certificates for a period of time. The set size N and the pseudonym change frequency are not specified and can be chosen by the vehicle manufacturer. A Pseudonymous Certification Authority (PCA) is responsible for the issuing of pseudonymous certificates $P_{cert_1} \ldots P_{cert_N}$ to the vehicles. Vehicular pseudonymous certificates P_{cert} can not be revoked. Pseudonymous certificates will only be issued to authenticated vehicles.

To identify a valid vehicle, each vehicular gateway is

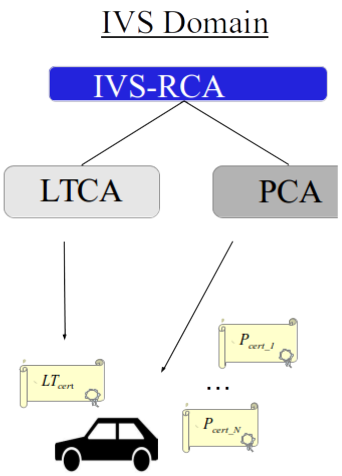


Figure 2. IVS PKI architecture promoted by the car2car communication consortium for Intelligent Vehicular Systems. This PKI consists of the Root Certification Authority (IVS-RCA), the Long Term Certification Authority (LTCA) and the Pseudonym Certification Authority (PCA)

equipped with a long term key pair and a corresponding vehicular long term certificate LT_{cert} for authentication purposes. A key pair and the according long term certificate LT_{cert} are issued to a vehicle at the beginning of the vehicle's lifetime. The issuing process of long term certificates is performed by the Long Term Certification Authority (LTCA). Validity periods of the LT_{cert} and the P_{cert} are not specified to date.

PCA and LTCA operate under a root CA called Intelligent Vehicle System root CA (IVS-RCA). To date, following revocation operations are provided: revocation of a LTCA- and PCA certification authority certificate and revocation of vehicular long term certificates LT_{cert}. The architecture of the IVS PKI domain is shown in Figure 2.

Long term certificates and pseudonymous certificates are implemented based on the new ETSI certificate format [5]. 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.

C. Using the IVS PKI for Road Side Units

The IVS PKI domain shown in Figure 2 is proposed by the car2car consortium for issuing certificates to RSU gateways as well. However, security and privacy requirements for vehicles and infrastructure components are not necessarily identical. In contrast to vehicles, RSUs (road work warning, traffic light, ...) 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, RSU gateways do not have to regard any active privacy concerns. As consequence, RSU gateways do not really need a set of valid pseudonymous certificates at each time. Instead, we propose that RSU gateways need only one Credential Certificate with a specific subject name adressing the RSU for each time frame. Due to security considerations for RSU gateways, see Section V, the validity period of credential certificates should be rather short.

Moreover, arising security weaknesses of the used security technology may be asessed differently by vehicle manufacturers on the one side and an infrastructure authority on the other side. However, the rules of operation for a PKI domain are defined 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 LTLs. So, each individual PKI domain can specify its own PKI policy for their specific needs. In addition, this multi-domain PKI architecture ensures that RSU unit gateways remain under control of the particular infrastructure authority.

The concept of a multi-domain PKI architecture without any superior root CA is not new and already mentioned in [16]. It has been applied globally for electronic passports for many years. Here, any 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 transportation 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 list is that each PKI domain has to securely mange is own LTL. More details concerning this issue can be found in Section IV-C.

IV. ITS PKI Concept

A. Role of Credential Certificates for Road Side Units

The primary use case for RSU gateways is the transmission of information, e.g., as DENM message to the vehicles using the wireless IEEE 802.11p channel. Due to integrity and authenticity reasons, these messages have to be signed. Therefore, the RSU gateways need specific keys and according certificates. RSUs do not have to regard any privacy concerns, as explained in Section III-C. Technically, this means that RSU gateways do not have to have pseudonymous keys and certificates. Instead, we propose that RSU gateways have only one valid credential key pair and one corresponding credential certificate at each time. Only in the transition phase between two certificate validity periods a RSU gateway has two valid credential certificates $C_{cert_{N-1}}$ and C_{cert_N}.

The RSU 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 credential certificate. By this a possible misuse of RSU gateways is made more difficult.

B. ITS PKI Architecture

As mentioned above, we propose that RSUs have only one credential key pair and one corresponding credential certificate C_{cert} at each time. The secret key corresponding to such a C_{cert} is used for signing RSU gateway 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, credential certificates should have a short validity period, for example one day. Thereby implicit revocation of C_{cert} becomes possible by not issuing new credential certificates to RSU gateways. The exact validity period of credential certificates have to be specified according to a detailed risk assessment concerning the addressed RSU type. For example RWWG are deployed for road works sites which usually are established for one or two days. It may be good practice then to issue a credential certificate with a validity period of a few days to a RWWG shortly before it is deployed.

For authentication purposes, e.g., to obtain credential certificates (for example on a daily basis) an infrastructure component requires a long term identification certificate LT_{cert}. These long term certificates LT_{cert} are issued by Long Term Certificate Authority (LT-CAs) during the enrolment of the RSU gateway. A long term certificate LT_{cert} is used within a certificate request for credential certificates towards the C-CA. We suggest that the credential key pair is generated within the secure element of the RSU gateway and the credential certificate is only issued after mutual authentication of RSU gateway and C-CA and only if the LT_{cert} of the RSU gateway is not revoked. Therefore, the LT-CA has to provide a CRL for revoked long term certificates LT_{cert}.

A LT_{cert} is only visible inside the ITS 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 ITS LT_{cert} 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 LT_{cert} should be at the order of years, e.g., five to six years for RSU gateways like RWWGs. As a rule, 5 to 6 years seems to be reasonable concerning useable cryptography or hardware security vulnerabilities. Due to different certificate issuing policies and certificate formats the LT-CAs and the C-CAs are attached to different root certification authorities, which are termed LT-RCA and C-RCA respectively.

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

Due to the short validity period of credential certificates of RSU gateways, the RSU gateways require an online communication channel, e.g., via GSM to receive new credential certificates.

C. Crypto Agility

Figure 4 shows how the validity periods of the certificates within the ITS PKI domain relate to each other. The validity 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 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 RSU gateways.
   - Assume that a LT-RCA root key pair (secret key: ${}^{RCA}LT_{SK\_1}$, public key: ${}^{RCA}LT_{PK\_1}$) is generated at time 0 of Figure 4. The secret key ${}^{RCA}LT_{SK\_1}$ is used to sign and issue a self-certified LT-RCA certificate ${}^{RCA}LT_{cert\_1}$, first. The certificate ${}^{RCA}LT_{cert\_1}$ is in state *active*.
   - The secret key ${}^{RCA}LT_{SK\_1}$ is used to sign CA certificates: ${}^{CA}LT_{cert\_1}$ and ${}^{CA}LT_{cert\_2}$.
   - The certificate ${}^{RCA}LT_{cert\_1}$ switches to state $passive$ at time point I when the next root key pair (secret key: ${}^{RCA}LT_{SK\_2}$, public key: ${}^{RCA}LT_{PK\_2}$) and according certificate ${}^{RCA}LT_{cert\_2}$ are issued. Now, the certificate ${}^{RCA}LT_{cert\_2}$ 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.

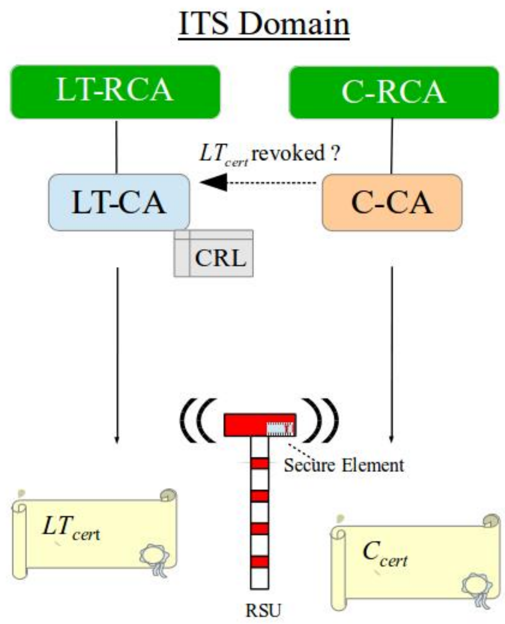


Figure 3. ITS PKI domain architecture. An ITS PKI domain consists of a LT-CA for issuing long term certificates LT_{cert} and a C-CA for issuing credential certificates C_{cert}.

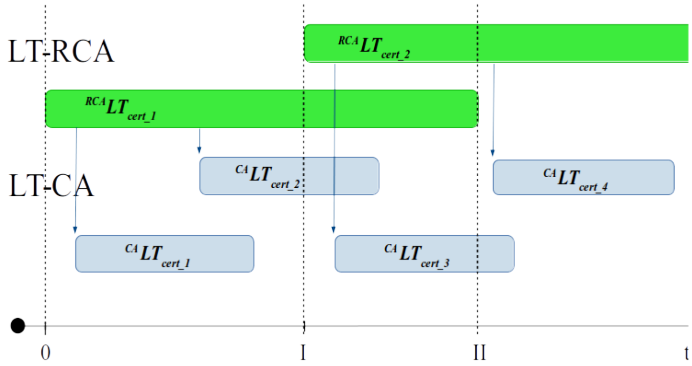


Figure 4. Certificate shell model. The validity period of a certificate is within the validity period of the issuing Certification Authority. E.g., the validity period of ${}^{CA}LT_{cert\_1}$ is within the validity period of ${}^{RCA}LT_{cert\_1}$

At time point II certificate ${}^{RCA}LT_{cert\_1}$ expires.

3) Certificate ${}^{RCA}LT_{cert\_2}$ is termed *Link Certificate* because it is signed with the former LT-RCA secret key ${}^{RCA}LT_{SK\_1}$.

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 a PKI have to follow the rules and instructions of the root CA. Therefore, changes of a cryptographic setting for a whole ITS PKI are prescribed by the root certification authority LT-RCA or C-RCA.

Changes to the following components are conceivable:

1) Elliptic Curve Domain Parameter (e.g., because longer key lengths are necessary)
2) Hash algorithm (e.g., due to new hash collision problems)
3) Signature algorithm (e.g., due to weaknesses in the used 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 perform the new algorithms.

The validity period of a LT_{cert} and a C_{cert} differ a lot. A LT_{cert} has a validity period of several years, whereas a C_{cert} has a validity period of few days at most. If the issuing PKIs C-CA and ITS-C-RCA have similar short validity periods with respect to the shell model, the cryptographic settings between LT_{cert} and C_{cert} can differ. In particular, shorter keys can be used for signing C_{cert} towards signing a LT_{cert}. Today, the ETSI certificate format only provides the NIST Elliptic Curve Domain Parameter P-256 [18] with 256 bits long secret keys. This key length is sufficient for the very near future. It is however highly probable that longer key length have to be used for long term certificates LT_{cert} in future.

D. Secure Trust Establishment between PKI domains

An examplary architecture of a multi-domain PKI with three PKI domains (ITS_I, IVS and ITS_II) is shown in Figure 5. 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 ITS domains ITS_I and ITS_II with the root CAs C-RCA_I and C-RCA_II managed by different infrastructure authorities. These two ITS domains issue credential certificates to RSU 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 the root CAs of the other 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., C-RCA_I manages the LTL for the ITS_I domain. Each PKI domain can individually define the needed rules that are sufficient to trust a separate PKI domain.

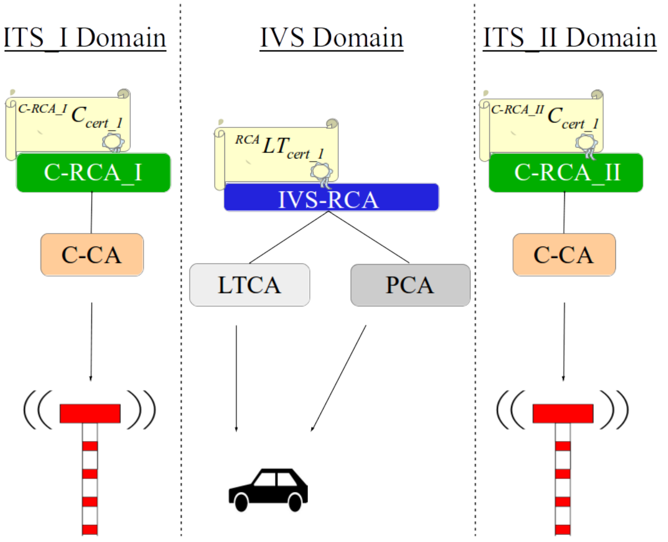


Figure 5. Examplary multi-domain PKI architecture with one IVS domain and two ITS domains: ITS_I and ITS_II.

To verify the authenticity of RSU gateway DENM messages in our examplary architecture, the vehicles have to know the root PKI certificates of the PKI domains ITS_I and ITS_II: ${}^{C-RCA\_I}C_{cert\_1}$ and ${}^{C-RCA\_II}C_{cert\_1}$. If the IVS PKI domain trusts in the ITS_I and ITS_II PKI domains the certificates ${}^{C-RCA\_I}C_{cert\_1}$ and ${}^{C-RCA\_II}C_{cert\_1}$ are elements of the LTL of the IVS PKI domain. 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 ITS_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 ITS_I and ITS_II, are not really required since no messages are exchanged between these domains. In our example the LTL of the two ITS domains just contain the ${}^{RCA}LT_{cert\_1}$.

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.

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 [19]. Therefore, further cryptographic ECC domain parameters (e.g., brainpool curves) should be added [20].

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 support crypto agility.

To date, ECDSA is specified as signature algorithm. ECDSA is an appendix signature. Because all entities (vehicles and RSU gateways) share only one wireless communication channel (IEEE 802.11p) it is important to restrict the length of CAMs and DENMs to avoid message collisions on the wireless IEEE 802.p channel at best. An alternative to appendix signatures are signatures with message recovery. For elliptic curve cryptography, e.g., Abes signature scheme with message recovery is applicable, see [21].

V. Security Requirements for RSU Gateways

RSU gateways operate in a potentially hostile environment. Attackers are able to physically manipulate these RSUs including the electronic gateway components. Also misuse of RSU gateways can not be excluded. First, these RSU gateways need a specific security functionality to resist active attacks and against removal of RSU gateways. But secondly, the PKI architecture has to appropriately regard this attack scenario as well. The idea is that a RSU gateway only acts in its designated role, e.g., as RWWG station, if it owns a valid credential certificate C_{cert}.

Moreover, security requirements for RSU gateways should be carefully analyzed and specified, e.g., in form of a Protection Profile (PP) according the Common Criteria.

The RSU gateways have to be satisfy following exemplary security requirements:

1) RSU gateways need a secure storage for cryptographic keys and have to be equipped with side channel resistant implementations of cryptographic algorithms.
2) RSU gateways are resistant against active attacks and removal from the RSU.
3) A RSU gateway is only able to act in his designated role if it owns a valid credential certificate.

If RSU gateways have specific resistance against 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.

VI. Conclusion

The proposed PKI of the Car2Car Communication Consortium for Intelligent Vehicular Systems (IVS PKI) does not regard all needs of RSUs. For this reason we suggest a multi-domain PKI to adequately address the requirements of vehicle manufacturers and infrastructure authorities. The PKI domains are cryptographically linked based on LTLs. In this paper the PKI architecture is only briefly described. Details have to be specified within the PKI policy documents of the different PKI domains. An open issue is the discussion of our multi-domain PKI proposal with stakeholders.

VII. Acknowledgement

The authors would like to thank Sandro Berndt and Arno Spinner from the Federal Highway Research Institute (BASt), our colleague Hans-Peter Wagner and the anonymous referees for valuable remarks.

References

[1] Car 2 Car Communication Consortium, “Mission, News, Documents,” 2015, https://www.car-2-car.org.

[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] ETSI, “Intelligent Transport Systems (ITS);Security; Security header and certificate formats, ETSI TS 103 097 V1.1.1,” 2013, http://www.etsi.org.

[6] 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.

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

[9] 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.

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

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

[12] 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. IEEE, 2008.

[13] 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.

[14] 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.

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

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

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

[18] 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

[19] 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.

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

[21] M. Abe and T. Okamoto, “A signature scheme with message recovery as secure as discrete logarithm,” in Advances in Cryptology-ASIACRYPT99. Springer, 1999, pp. 378–389.